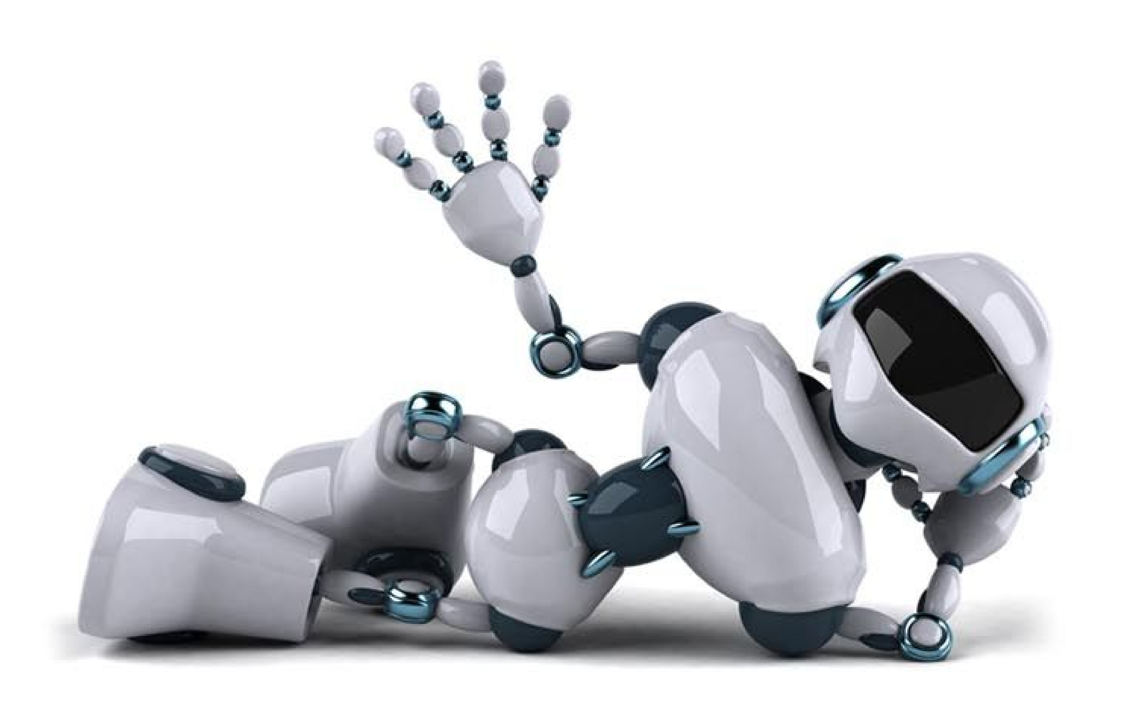


spanning tree protocol

ESX and ESXi

Auto-secure

REGEX

ieee





March 2011

NetworkSet

NetworkSet Magazine

أول مجلة عربية مجانية تختص بأمور الشبكات

www.Networkset.net



المحتويات

الأبحاث العلمية أم المحتوى العربي

قد لايخفى على الجميع أن المحتوى العربي على الأنترنت والمراجع العلمية بشكل عام تشكل عشرة بالمئة فقط من المراجع الموجودة بلغات أخرى وتشير بعض الدراسات أن المحتوى العربي على الأنترنت يشكل ثلاثة بالمئة فقط ؟؟؟...

نعم أخي العزيز هذا هو حالنا العربي على الأنترنت ألاف المواقع العربية والمدونات والمنتديات وفي الآخر ثلاثة بالمئة فقط ومازال اغلبنا نائم ينتظر اليوم الذي يستيقظ فيه ويجد كل مايطلبه من علوم متوفر على الأنترنت وأكيد أن هذا اليوم لن يأتي طالما مازال تفكيرنا وهدفنا هو إيجاد العمل والفرصة المناسبة وطالما هناك زر في أجهزة التشغيل يدعى (نسخ لصق) فمن خلال متابعتي لأحد أشهر المنتديات العربية في مجال الشبكات أجد ألاف الأعضاء الذين يمرون على المنتدى ويستفيدوا من وجود بعض الأعضاء الذين يعملون بدون مقابل ويبدأ أستهلاك كل ماهو موجود ومفيد ويأخذوا هذه الشهادات الورقية ليضعوها في سيرتهم الذاتية ليختفوا بعدها من دون رجعة فهدفهم قد تحقق وهو سيرة ذاتية وعمل يحقق لهم غاية الأستهلاك الوقائي.

ومن ناحية أخرى نجد بعض المؤسسات والحكومات العربية التى تنفق ملايين الدولارات لبناء مراكز أبحاث مجهزة بأفضل الوسائل العلمية لكي يبدؤا أكتشاف أبحاثهم العلمية المزعومة ومن هنا أطرح سؤال في غاية الأهمية, ياترى من سوف يعمل في هذه المراكز وعلى أي المراجع سوف يعتمدوا ؟ المراجع محلولة فلقد أتفقنا أن المراجع العربية شبه معدومة وسوف تكون المراجع الأنكليزية هي المكان الوحيد لهم و بالتالي سوف نستنتج شيء في غاية الاهمية وهو ضرورة وجود باحثين ومطورين يجيدون اللغة الانكليزية كلغة أم بينما الشخص الذي لايجيد اللغة الأنكليزية بطلاقة فمكانه عمل إداري ممل محصور في أربع جدران لأنه ببساطة ليس من الأقلية التى يمكنها أن تستفيد من هذه المراكز.

بالنسبة لي أعتبر هذا الشيء في غاية ***** لأن التفكير الحقيقي الآن يجب أن ينصب في أستهداف الاكثرية وهي التى تتحدث اللغة العربية لأن صعود درج العلم يجب أن يكون درجة درجة وليس عشر درجات فأنتم تحاولوا القفز إلى مراكز لن تصلوها أبدا لأنكم تستهدفوا الأقليات وهذه الاقليات مهما كان درجة ذكائها ومستواها العلمي سوف تبقى أقلية بينما تركتم الأكثرية لتجلس وتنتظر.......لذلك أنا أتوجه إليكم ومن خلال منبري الصغير هذا توقفوا عن دعم الأبحاث العلمية قليلا وفكروا في دعم المحتوى العلمي فهو البوابة التى وصلت لها جميع الأمم إلى ما هي عليه الآن وليس في صرف الملايين على أستيراد معدات نحتاج فيها فنيين من عندهم لكي نتعلم كيف نستخدمها!!!. إلى متى هذا الأستهتار؟ وإلى متى سوف نبني دراسات فاشلة ؟ وأستحلفكم بالله أليس صرف مبلغ عشرة ملايين دولار يمكن أن يحول المحتوى العربي من ثلاثة بالمئة إلى ثلاثين بالمئة في فترة أقل من عام ؟!!!!....أليس صرف مبلغ عشرة ملايين على دعم المناهج العلمية في الجامعات العربية سوف يخرج لنا ألاف الباحثين والمفكرين؟!...

أخي العزيز أختي العزيزة أتركوا سوء بناء الدراسات من قبل المؤسسات والحكومات العربية وساهموا في بناء عزة عالمنا العربي فنحن الاكثرية ونحن من سوف يبني هذا التاريخ وحاولوا ان توجهوا تفكيركم نحو حلم عربي واحد وكبير وثقوا بأن شخص واحد يمكنه أن يغيرا العالم ويمكن ان يكون هذا الشخص هو أنت !... لكن إذا تعلمت كيف تستفيد من قدراتك ووقتك بشكل صحيح في صالح بناء محتوى عربي نورثه للأجيال التى من بعدنا وخصوصا أن عجلة العلم كل يوم تصعد مئات الدرجات ونحن مازلنا نحاول صعود الدرجة الأولى منها وهو بناء المحتوى..... ودمتم بود

أيمن النعيمي

الرخص وطريقة إعدادها على أجهزة سيسكو

أحمد الشحات

هذا المقال هو الجزء الثانى من مقالة نشرت فى المجلة فى العدد قبل السابق (أى فى عدد يناير 2011) بعنوان – الرخصة و طريقة إعدادها على أجهزة سيسكو – ، وتكملة لما بدأته فإن لى ملاحظة :

كل node تكون لها رخصة واحدة node license unit تأتي معها، وكما قلنا سابقا أن ال Node هو cucm ، أما كل جهاز فيكون له عدد ثابت من ال Licenses units تختلف بإختلاف نوع الجهاز، و كما قلنا سابقا أن الجهاز 7970 يحتاج 5 رخص و الجهاز 7961 يحتاج أربعة وهكذا.

Cucm يحتوى على starter license تأتى مع الجهاز الجديد التي يمكن إستخدامها للبدء فى عملية التحميل للبرنامج على cucm . النظام يقوم بعملية الكتابة على ال starter licenses عندما نحصل على الرخصة الدائمة permenant license ونقوم برفعها لل cucm .

للحصول على الرخصة الدائمة permanent license نستخدم Product Authorization Key(PAK) الذي يأتي مع المنتج، ندخل Product Authorization Key(PAK) الذي تم الحصول عليه مع المنتج أو بواسطة التليفون فى License Registration web tool الموجود فى الرابط التالي http://www.cisco.com/go/license، ونضغط Submit ونتبع التعليمات.

و يجب أن ندخل ال MAC Address الخاص بال NIC o Ethernet الخاص بأول node من cucm فى CLUSTER وعدد الأجهزة وعدد ال nodes أيضا، وأيضا ندخل عنوان البريد الإلكتروني لكي تتلقى الرخص عليه Licenses .

cisco

Search Go

Solutions | Products & Services | Ordering | Support | Training & Events | Partner Central

HOME

Product License Registration

Support

Product License Registration

Enter a PAK Number | Step 2 Validate Features | Validate Features | Step 3 Designate Licensee | Designate Licensee | Step 4 Finish and Submit | Finish and Submit

Licenses Not Requiring a PAK

If you do not have a Product Authorization Key (PAK), please click here for available licenses.

Available licenses include Evaluation/Demo Licenses, Cisco ASA 3DES/AES, PIX Firewall 3DES/AES and DES Encryption, Cisco Services for IPS, and Cisco Unified Communications Manager Version Upgrade licenses.

Product Authorization Key (PAK)

Enter the Product Authorization Key (PAK) below exactly as it appears on the label that accompanied the Cisco Information Packet.

Product Authorization Key (PAK): *

Enter one value at a time including dashes

Go Back | SUBMIT

RMA License Transfer

بعد عمل التعليمات السابقة فإن شركة سيسكو ترسل ملفات الرخص (License Files) إليك بواسطة الإيميل الذي قمت بوضعه سابقا، ويكون شكل إسم الرخصة (CCM<timestamp>.lic).

مثال حقيقى (CCM20091214113826681.lic).

ملحوظة مهمة جدا:

يمكن تغيير إسم الرخصة لو لم يعجبك الإسم و لكن لايمكن تغيير المحتوى على الإطلاق، ويمكن فتح الرخصة بواسطة المفكرة ورؤية محتوياتها و لكن لاتعدل فيها.

ملحوظة أخرى:

يمكن أن يطبق ملف رخصة و احد على أكثر من node فى ال cluster الذي أعمل عليه وسنرى ذلك لاحقا.

يجب رفع الرخصة إلى السيرفر الذي قمت بإرسال ال MAC Address له، و عندها سيبدأ السيرفر بالعمل.

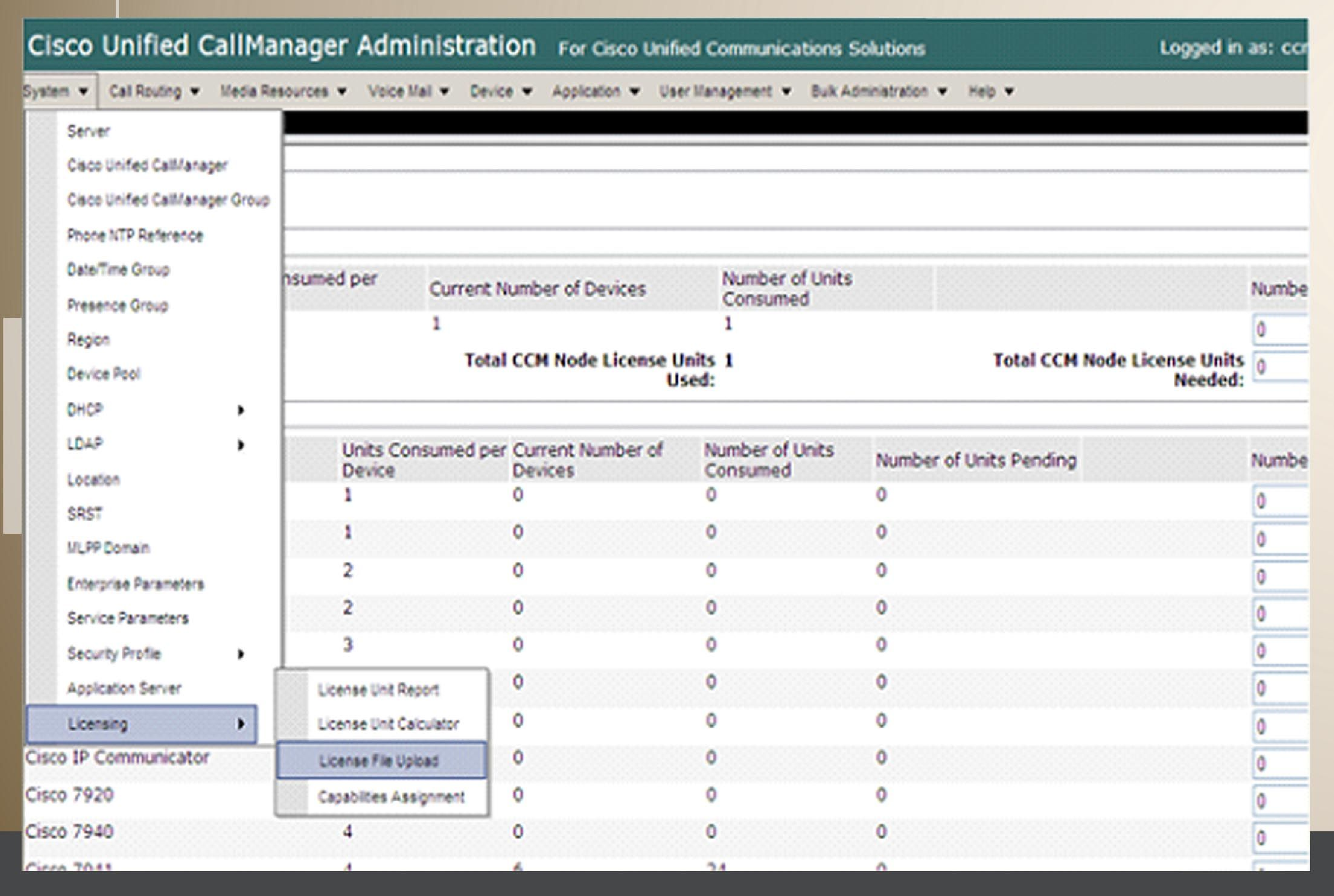
ملحوظة : يمكن إستخدام الرخص الموجودة فى ملف الرخصة الذي حصلت عليه من سيسكو فى نفس ال cluster فقط.

كيفية تحميل ملف الرخصة على CUCM

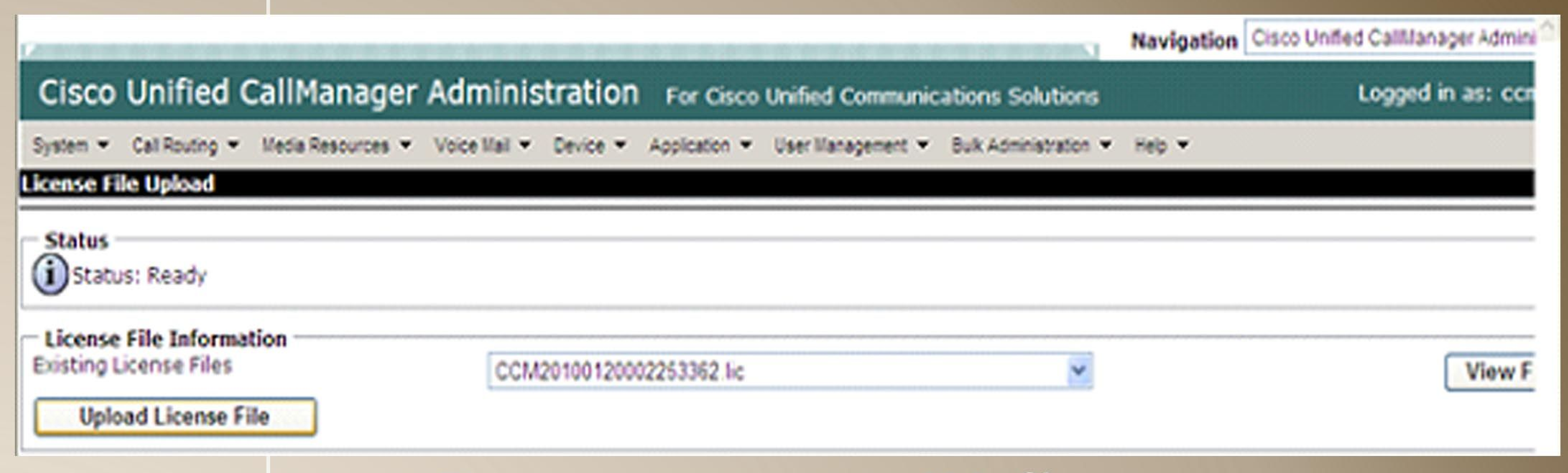
ملحوظة يتم تحميل ال Licenses على أول Node فى ال CLUSTER فقط، يعني مثلا على CUCM PUPLISHER

أما ال Subscribers فلا يتم تنزيل أى Licenses عليها.

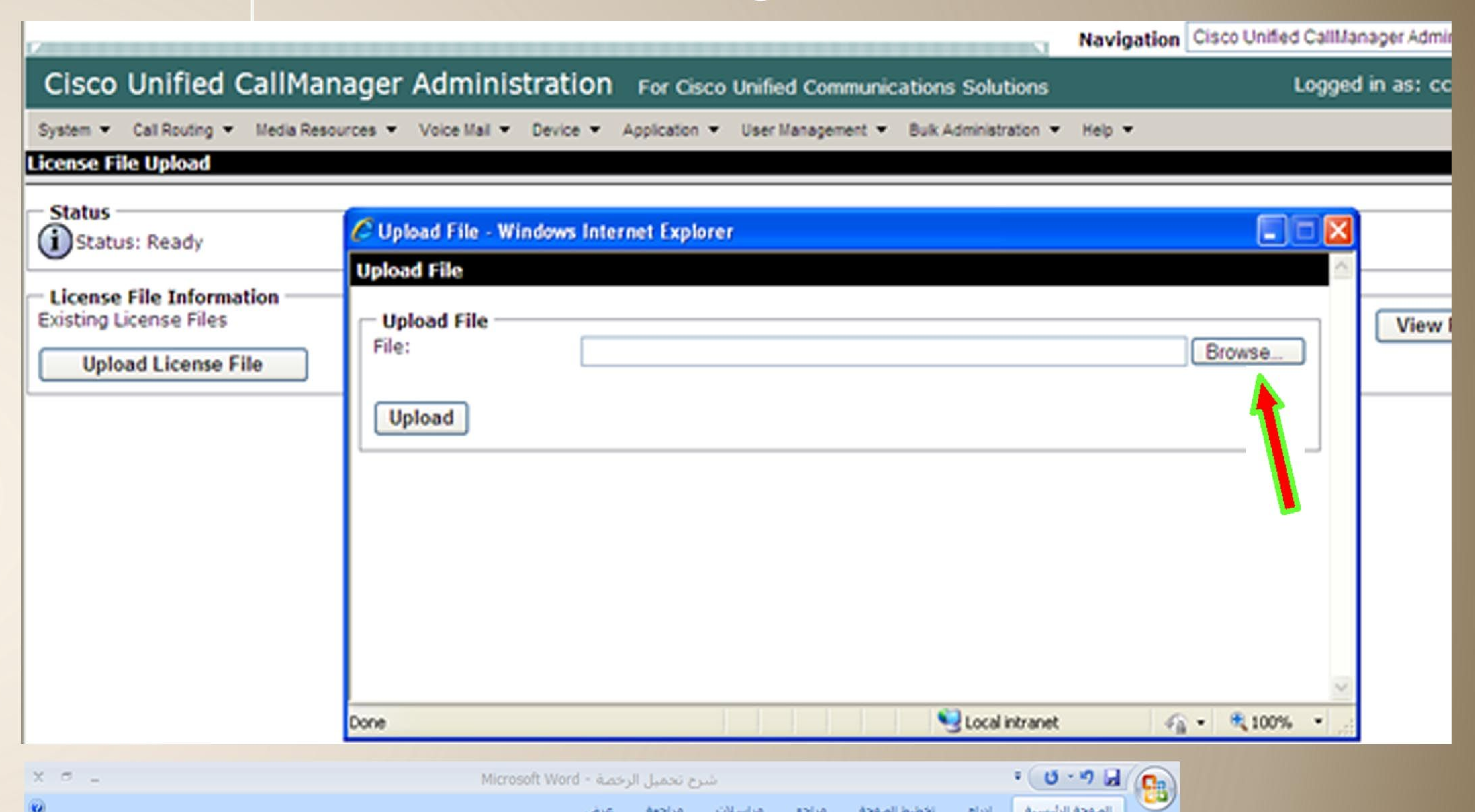
.System > Licensing > License File Upload



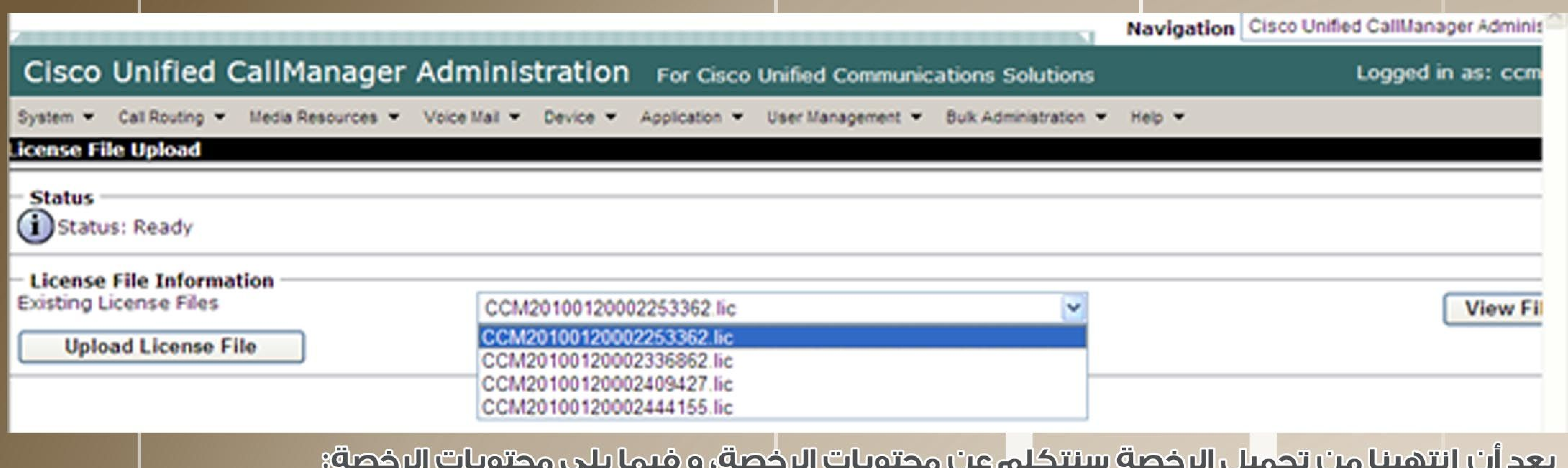
طبعا الLicense موجودة لأنني لن أقوم بحذفها من أجل التجربة، أما فى الواقع ستجد هذا المربع فارغ و تضغط علىUpload License file لتحميل الرخصة الجديدة.



ولرؤية محتويات الرخصة نضغط علىVeiw file ، و لتنزيل رخصة جديدة نختارBrows ثم نحدد المسار.



نحدد الرخصة المطلوبة ثم نختار Upload .



بعد أن إنتهينا من تحميل الرخصة سنتكلم عن محتويات الرخصة، و فيما يلي محتويات الرخصة:

سأضع نموذج لرخصة CUCM ونموذج لرخصة IP PHONE

1* نموذج رخصة الNODE

\ INCREMENT CCM_NODE cisco 6.1 permanent uncounted

VENDOR_STRING = <Count>1</Count><OrigMacId>00215ABBFD92</OrigMacId>

\ <<LicFileVersion>1.0</LicFileVersion

\ HOSTID = 002655ad4de0

\ <NOTICE = "<LicFileID>20091214113826681</LicFileID><LicLineID>1</LicLineID

\ PAK>1156J5028D9</PAK>" SIGN = "0618 88F6 653B 8136 985E 503E>

\ A1A8 97BF 9FBD D196 2629 E598 C90B 9621 9F06 1357 2310 E040

"14D4 A29F C50B A5E7 6589 3D64 6668 4C8B 03CD 947C 0552 E2CD

\ INCREMENT SW_FEATURE cisco 6.1 permanent uncounted

VENDOR_STRING = <Count>1</Count><OrigMacId>00215ABBFD92</OrigMacId>

\ <<LicFileVersion>1.0</LicFileVersion

\ HOSTID = 002655ad4de0

\ <NOTICE = "<LicFileID>20091214113826681</LicFileID><LicLineID>2</LicLineID

\ PAK>1156J5028D9</PAK>" SIGN = "1DE2 CD17 6102 C277 341A 2A29>

\ 26B4 CB2F 14A1 57C6 4ABB C55D B19C 67F2 506D 0CF8 79DD 8D5B

"9F1F BDC6 D0F1 42BC 7BF2 70C1 E708 ABF2 9005 A86B 66B2 53EF

معنى الجملة INCREMENT CCM_NODE cisco 6.1 permanent uncounted انها رخصة غير منتهية

معنى الجملة VENDOR_STRING = <Count>1 أنها رخصة واحدة فقط، لجهاز واحد

معنى الجملة HOSTID = 002655ad4de0 هذا هو الMAC ADD

2* شكل رخصة IP PHONE

INCREMENT PHONE_UNIT cisco 6.0

\ permanent uncounted

VENDOR_STRING=<Count>1000</Count><OrigMacId>000BCD4EE59D</OrigMacI

<d

\ <LicFileVersion>1.0</L icFileVersion>

HOSTID=000bcd4ee59d

NOTICE="<LicFileID>20050826140539162</LicFileID><LicLineID>2

\ <LicLineID/>

\ PAK></PAK>" SIGN="112D 17E4 A755 5EDC F616 0F2B B820 AA9C>

\A36F B317 F359 1E08 5E15 E524 191566EA BC9F A82B CBC8 0313

"4CAF 2930 017F D594 3E44 EBA3 04CD 01BF 38BA BF1B

هذه رخصة ل 1000 تليفون

أتمنى أن أكون قد وفقت فى توصيل المبادىء إليكم

والله ولي التوفيق

عمرو يحيى

AAA

أهلا بالقراء الأعزاء وأسف لعدم كتابتى لمقالات خلال الفترة الماضية نظرا لإمتحاناتى، وللظروف التى مرت بها مصر الحبيبة حفظها الله وحفظ كل البلدان العربية وحدة واحدة وأمة واحدة.

موضوع الـ AAA

هى عملية هامة جدا فى عملية الحماية للشبكات حيث أنها توفر ثلاث مزايا غاية فى الروعة لحماية الشبكات وهذه المزايا الثلاث هى المكونة لإختصار الـ AAA أو Triple A .

Authentication, Authorization, and Accounting

Authentication

هى المرحلة الأولى حيث أنها العملية التى يتم من خلالها إثبات أن المستخدم أو المدير هو الشخص الصحيح أو المفترض به

أن يكون. والغرض من هذه العملية هى التأكد من عدم دخول أشخاص غير مسموح لهم بالدخول وتتم هذه العملية بإستخدام أوراق الإعتماد (Credentials). وتشبيها لهذه العملية هى شرطة المطار حيث تسمح بالدخول حسب أوراق الإعتماد وتمنع الأشخاص الضارين وأمثلة أوراق الإعتماد كثيرة منها:(Passwords, one-time tokens, digital certificates).

Authorization

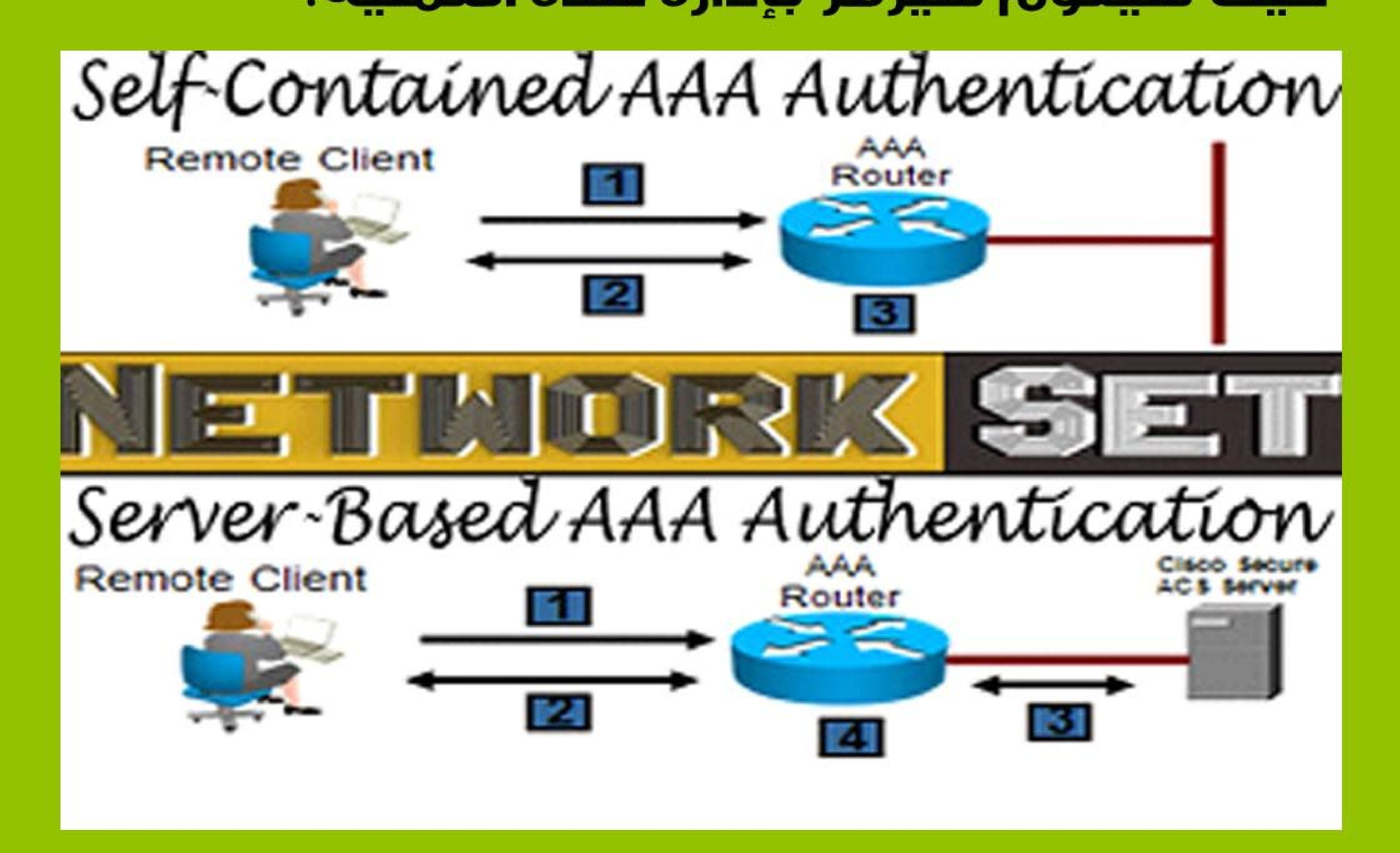
هى المرحلة الثانية حيث أن كل مستخدم مسموح له بالدخول يمتلك صلاحيات محددة لا يستطيع أن يتعداها و يقوم بالتعامل مع الأجهزة من خلال هذه الصلاحيات فتحدد الأماكن التى يمكن الدخول عليها وصلاحيات التعامل مع البيانات، ومثال لها المنظومة العسكرية حيث كل رتبة لها الصلاحيات المحددة لها.

Accounting

هى المرحلة الثالثة وهذه العملية تسجل الأفعال وما قام المستخدم أو المدير بعمله خلال إستخدام الأجهزة أو الدخول على الشبكة كلٌ حسب صلاحياته فهى تراقب المستخدم للشبكة وأيضا تسجل فترة دخوله ومعلومات أخرى تفيد فى الحماية ومنها Security Audit و التى عن طريقها يتم معرفة الإختراقات فى الشبكة وعلاجها، وهذه الخاصية مهمة جدا حيث تستخدم فى عملية التفتيش عند إختراق الشبكة حيث يتم تتبع كل مستخدم وما قام بفعله خلال الفترة التى حدث بها الإختراق ومن ثم يتم معرفة الثغرة أو الشخص الذى قام بالإختراق.

لكن قبل التعمق فى ال (AAA) هناك سؤال يتبادر إلى الأذهان، وهو لماذا إتجهنا إلى ال (AAA)؟ وما المرحلة التى سبقته؟

الإجابة بإختصار أنه قبل إستخدام ال (AAA) تم الإعتماد على ال (Local Database) حيث يخزن على كل جهاز جميع المستخدمين وكلمات السر الخاصة بهم، ومع زيادة الأجهزة وكبر حجم الشبكات أصبح من الصعب الإعتماد على ال (Local Database) وتم التوجه إلى (AAA) حيث سيقوم سيرفر بإدارة هذه العملية.



أنواع سيرفرات الـ (AAA)

- RADIUS

سنتحدث عنه بنظره عامة كبروتوكول ثم نظرة عن كثب كسيرفر

هذا البروتوكول قد تم تطويره بواسطة شركة ليفينغستون (Livingston Enterprises Inc.) وأصبح بعد ذلك (One of IETF Standards). وبسبب طبيعة تكوينه الواسع، ظهرت له إستخدامات جديدة وعديدة منها الإنترنت، والشبكات الداخلية، واللاسلكية، وخدمات الإيميلات المتكاملة. ولكثرة أنواع الشبكات التى يتعامل معها ظهرت فى إستخداماته قاعدة كبيرة من الأجهزة والخدمات منها Modems, DSL, Access points, VPNs, Network ports, Web servers

يعتمد هذا البروتوكول فى تكوينه على (Client/Server) من الطبقة السابعة (Application Layer) بإستخدام ال (UDP Transport) ولذلك يستوجب ذلك وجود كل من: RADIUS client component

RADIUS server

(RADIUS) وهى إختصار لـ Remote Authentication Dial in User Service **غالبا يعمل كسيرفر فى بيئة الأنظمة (Linux, UNIX, Windows NT) ويتم الإتصال بين جميع المستخدمين أو ال (Clients) مع ال (Remote Access Server (RAS)) وهو ال (RADIUS Server) للسماح لهم بالدخول للشبكة.**

ولن أتطرق إلى عمليات ال (Authentication) و (Accounting) و (Roaming) فقد تم التحدث عنها بشكل أعمق فى عدد سابق، فالهدف من هذا المقال الحديث بشكل عام على ال (AAA).

• TACACS

هذا إختصار ل Terminal Access Controller Access-control System (TACACS)

هذا السيرفر من نوع (Remote Access Server (RAS)) ليحدد إذا كان المستخدم له حق الدخول على الشبكة أو لا، فقد قدم (TACACS) فى البداية يستخدم أى من (TCP) أو (UDP). ثم قامت شركة سيسكو بتطويره فقدمت عام 1990 (Extended TACACS (XTACACS)).

وقد أتاح ال (TACACS) السماح للمستخدم (Client) عن طريق الباسوورد و إرسال ال (Query) إلى (TACACS Server)، وقد إستبدلته (CISCO) ب (TACACS+) المستخدم حاليا بكثرة والمكافئ لل (RADIUS) ولكنه و على العكس منه يستخدم (TCP) و (UDP).

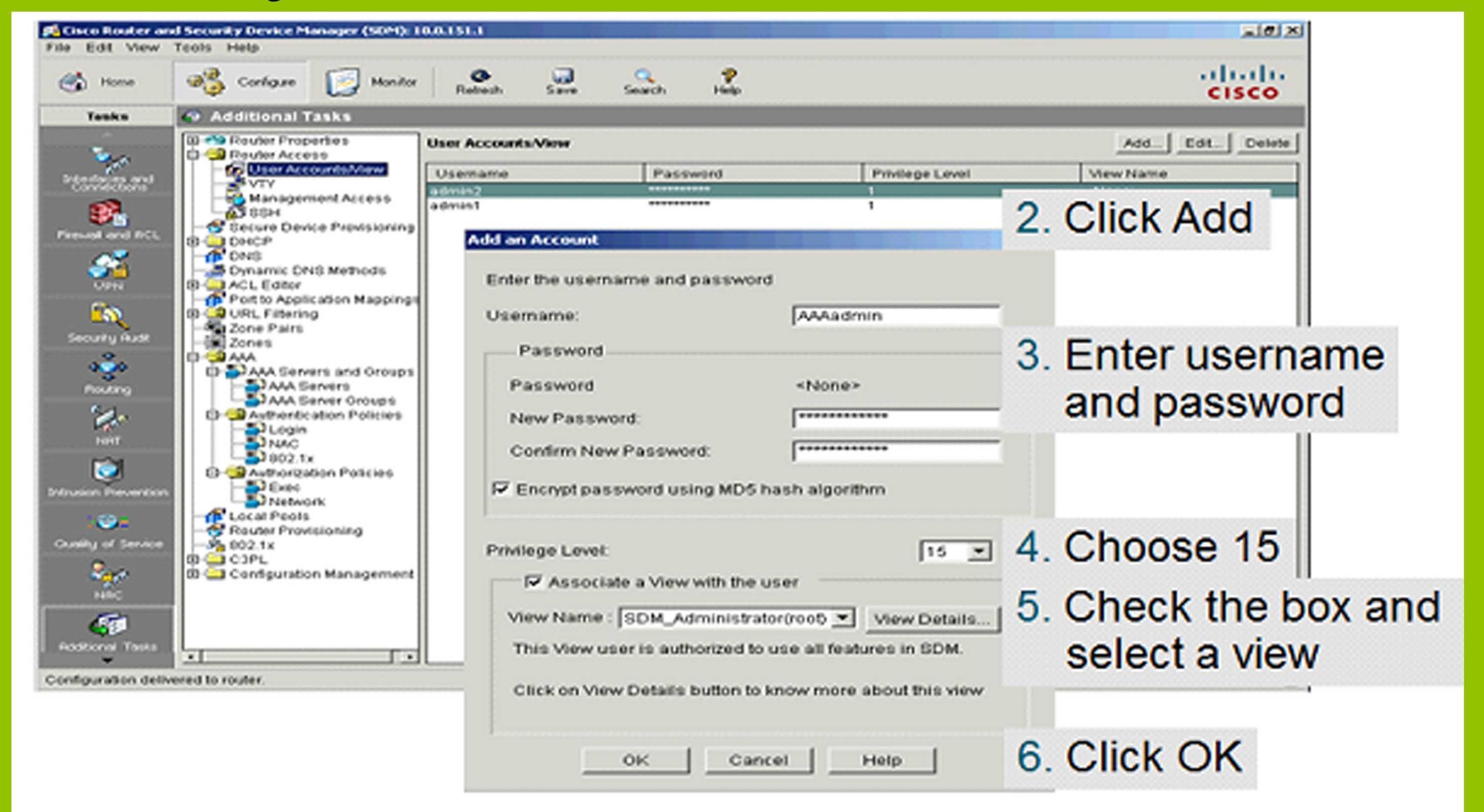
وهذه مقارنة بين (TACACS+ & RADIUS)

	TACACS+	RADIUS
Functionality	Separates AAA according to the AAA architecture, allowing modularity of the security server implementation	Combines authentication and authorization but separates accounting, allowing less flexibility in implementation than TACACS+.
Standard	Mostly Cisco supported	Open/RFC standard
Transport Protocol	TCP	UDP
CHAP	Bidirectional challenge and response as used in Challenge Handshake Authentication Protocol (CHAP)	Unidirectional challenge and response from the RADIUS security server to the RADIUS client.
Protocol Support	Multiprotocol support	No ARA, no NetBEUI
Confidentiality	Entire packet encrypted	Password encrypted
Customization	Provides authorization of router commands on a per-user or per-group basis.	Has no option to authorize router commands on a per-user or per-group basis
Confidentiality	Limited	Extensive

AAA using SDM

برنامج (Security Device Manager (SDM)) و هو خاص بسيسكو وله مزايا عديدة منها الخاصية الأكثر من رائعة (Security Edit)، ومنها أيضا تطبيق ال (AAA) بكل سهولة.

Select Configure > Additional Tasks > Router Access > User Accounts/View



Cisco Secure ACS



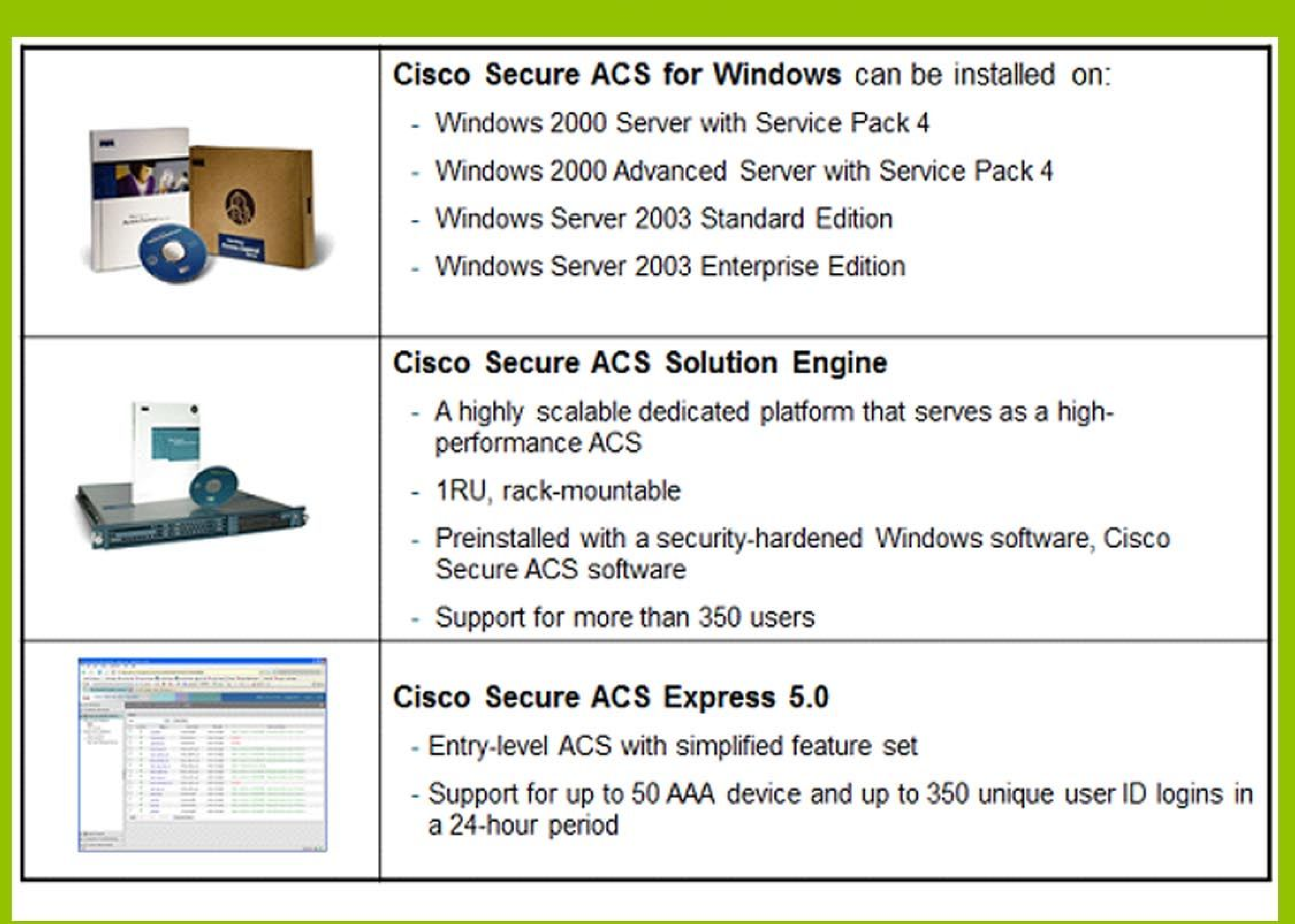
إختصار لـ (Access Control System):

هو أحد منتجات سيسكو قد يكون عبارة عن سوفت وير يعمل على أنظمة تشغيل مختلفة أو هاردوير قائم بذاته يوفر تحكم وإدارة للدخول لموارد الشبكة مع المجموعات المتنوعة من الأجهزة ومجموعات المستخدمين، وطرق أخرى للدخول عن بعد لفرض الحماية الكافية للشبكة، ويقلل من ال VPN، ويسمح بالتحكم عن بعد، ويتيح التعامل مع جهود الإدارة والتحكم على مديرى الشبكات.

ويستقبل البيانات TACACS+ & RADIUS من بروتوكولين مختلفين هما:

- (Easy-to-use) ويزود دخول سهل بواسطة troubleshooting يوفر مراقبة تامة للشبكة وتقارير عنها.
- وأيضا (Web-based GUI)

وهذه قائمة بأنواعه ومزاياه



	Cisco Secure ACS for Windows can be installed on: - Windows 2000 Server with Service Pack 4 - Windows 2000 Advanced Server with Service Pack 4 - Windows Server 2003 Standard Edition - Windows Server 2003 Enterprise Edition
	Cisco Secure ACS Solution Engine - A highly scalable dedicated platform that serves as a high-performance ACS - 1RU, rack-mountable - Preinstalled with a security-hardened Windows software, Cisco Secure ACS software - Support for more than 350 users
	Cisco Secure ACS Express 5.0 - Entry-level ACS with simplified feature set - Support for up to 50 AAA device and up to 350 unique user ID logins in a 24-hour period

لا أعتقد أنه يسعنى الوقت لذكرها قد أتمكن من عرضها فى (AAA) وهناك تطبيقات وخفايا كثيرة يمكن تطبيقها على

موضوعات قادمة بإذن الله وأتمنى أن أكون قد وفقت فى عرض الموضوع بنظرة شاملة تمكن القارئ من معرفة (AAA) وأيضا لا أود أن أطيل عليكم حتى لا يشعر القارئ بالملل.

AUTO-SECURE

ميـزة من سيسكـو تضعك مع محترفي الأمن والحماية





قد يتطلب منك حماية روتر على الشبكة بشكل جيد القيام بتنفيذ أكثر من أمر وهذا يشمل تفعيل وتعطيل بعض الخدمات الموجودة على الروتر من أجل رفع مستوى الأمن على الروتر وطبعا هذا يتطلب خبرة جيدة مع نظام التشغيل وأوامره, لذا قامت سيسكو بأضافة ميزة لهذا الأمر ويتم تفعيلها من خلال أمر يقوم بتنفيذ كل خيارات الأمن المتاحة على أجهزتها وهو الأمر Auto secure

فمنذ الأصدار 12.3 تم أضافة ميزة لأجهزة سيسكو تسمح لرفع مستوى الأمن والحماية على أجهزتها وبسرعة كبيرة جدا ومن خلال أمر واحد تقوم بكتابته في الـ Privileged Mode ويعد هذا الأمر مدعوم في عدة أجهزة ومن بينها الأجهزة التالية 800, 1700, 2600, 3600, 3700, 7200, 7500 ومن ناحية أخرى أتاحت سيسكو هذا الأمر من أجل الأشخاص المبتدئين في مجال سيسكو ولاتوجد لديهم خبرة في التعامل مع أجهزتها ومع نظام التشغيل IOS الخاص بها وذلك من خلال عمل Dialog بسيط يسألك فيه بعض الأسئلة أي أن الأمر شبيه بالـ initial configuration dialog الذي نراه عند تشغيلنا للروتر أول مرة لكن هنا الأسئلة سوف تكون متعلقة بالأمن والحماية فقط لذا لنشاهد بعض الأمثلة الواقعية وقبل أن أبدا لنكتب الأمر ونضع بعدها إشارة أستفهام لكي نرى ماهي أمكانيات هذا الأمر وماهي الـ Plan المتاحة :

```
Cisco's IOS
Router#auto secure ?
forwarding     Secure Forwarding Plane
full           Interactive full session of AutoSecure
login          AutoSecure Login
management     Secure Management Plane
no-interact    Non-interactive session of AutoSecure
ntp            AutoSecure NTP
ssh            AutoSecure SSH
tcp-intercept  AutoSecure TCP Intercept
<<cr
```

وكما يتضح لكم هناك ثمانية خطط أو Plans ولكل Plan هناك شرح بسيط عنها يحدد نوعية الأسئلة التى سوف يتم سؤالك عنها ولو لم تختار أي واحد منها وقمت بكتابة الأمر فقط فسوف يتم تفعيل خيار الـ Full كخيار Default للـ AutoSecure لنأخذ هذا المثال البسيط وهو خاص بي الـ Login ولنشاهد الأسئلة المطروحة :

Cisco's IOS

```
Router>en
Router#auto secure login
— AutoSecure Configuration —
*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***
AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.
Gathering information about the router for AutoSecure
Is this router connected to internet? [no]: no
Enable secret is either not configured or
is the same as enable password
Enter the new enable secret******:
Confirm the enable secret******* :
Enter the new enable password*******
Confirm the enable password*******:
Enter the username: networkset
Enter the password******:
Confirm the password******:
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters
Blocking Period when Login Attack detected: 200
Maximum Login failures with the device: 3
Maximum time period for crossing the failed login attempts: 180
!
end
Apply this configuration to running-config? [yes]: yes
Applying the config generated to running-config
#Router
```

كما تشاهدون معي أن السؤال الأول كان حول معرفة هل هذا الروتر متصل مع الأنترنت أم لا وقد أجابت بلا ولو أجبت بنعم كان طلب مني تحديد أي المنافذ متصل مع الأنترنت وبعدها تم سؤالي حول كلمات السر واسم المستخدم الخاص فيني وعدد مرات التى سوف أسمح فيها بتسجيل خاطئ لكلمة السر والفترة الزمنية التى سوف أسمح فيها بكتابة كلمة السر مرة رابعة والخ..... وطبعا أخر سؤال سوف يكون حول أضافة هذه الأوامر وتطبيقها على الروتر.

وطبعا نفس الشيء لو تم أختيار خطة أخرى فلو مثلا أخترنا خيار الـ Full فسوف تكون الأسئلة مختلفة بعض الشيء ومن بينها وضع الـ Banner واسم المستخدم وكلمة السر وأسم الدومين والخ......

كلمة لآخيرة هناك أمر مشابه لهذا الأمر لكن مع الـVoice وهو خاص بي الـ QoS.

أحمد مصطفى

CISCO Configuration Professional وطريقة توصيله مع الـ GNS3

هل إنتهي عصر الـ SDM؟

وهل إحتل ال CCP عرش ال GUI كلية؟

وهل بدأت سيسكو عهداً جديداً في التضييق علي برامج المحاكاة؟

هذا وغيره من الأسئلة ما سنتناوله في هذه المقالة بإذن الله.

توقفت سيسكو عن تحديث برنامج ال SDM (CISCO Security Device Manager) منذ عام 2008، وتوقف البرنامج عند الإصدار V2.5. ثم في عام 2010 أصدرت سيسكو النسخة الأولي من برنامج Cisco Configuration Professional أو إختصاراً CCP.

البرنامج لا يختلف كثيراً عن ال SDM في واجهته الرسومية، ولكن عملية ال Configuration أصبحت أفضل وأكثر مرونة، ولكنه يختلف عن ال SDM في الآتي:

١* متطلبات التشغيل أصبحت أكبر من ال SDM وهذه يمكن تلخيصها في الآتي:

System Component	Requirement
Processor	2 GHz processor or faster
Random Access Memory	1 GB DRAM minimum; 2 GB recommended
Hard disk available memory	400 MB
Operating System	Any of the following: • Microsoft Windows 7-32 and 64 bit • Microsoft Windows Vista Business Edition • Microsoft Windows Vista Ultimate Edition • Microsoft Windows XP with Service Pack 3-32 bit • Mac OSX 10.5.6 running Windows XP using VMWare 2.0
Browser	Internet Explorer 6.0 or above
Screen Resolution	1024 X 768
Java Runtime Environment	JRE versions 1.6.0_11 up to 1.6.0_21 supported
Adobe Flash Player	Version 10.0 or later, with Debug set to "No"

وكما نلاحظ أن قدرة ال Processor وال RAM زادت، وهذا أيضاً يزيد تبعاً لنسخة ال CCP. كما نلاحظ أن سيسكو لا تدعم باقي أنظمة التشغيل مثل ال LINUX فالبرنامج بنسخته موجود في صورة .EXE وهو ما لا تدعمه باقي أنظمة التشغيل، كما نلاحظ أيضاً أن البرنامج ذاته عبارة عن صفحة ويب لا تعمل إلا على ال Internet Explorer فقط دون باقي المتصفحات.

* النقطة الأهم أن البرنامج أصبح لا يدعم كثير من الأجهزة التي كان يدعمها ال SDM.

. فهو لا يدعم أغلب الأجهزة التي يدعمها برنامج المحاكاة GNS3 ، اللهم إلا نسخة 7200، وهذا يجيب على التساؤلات التي طرحناها في البداية،

أننا مازلنا نحتاج إلي ال SDM لعمل الإعدادات Configurations اللازمة لبعض الموديلات، وأن ال CCP لم يتربع على عرش الـGUI كلية على Configuration.

3* ومن الإختلافات أيضاً ، أن البرنامج يأتي في صورتين:

أ* نسخة Express وهي نسخة صغيرة الحجم للتسطيب علي الروتر.

ب* نسخة Professional وهي النسخة التي يتم تسطيبها علي ال PC.

على عكس الSDM ، حيث كانت النسخة الواحدة يمكن تسطيبها علي الروتر وال PC معاً.

❄4 يوفر البرنامج أيضاً نسخة Demo. وهي نسخة تجريبية تعطيك الحرية للتدريب علي البرنامج في بيئة محاكاة، بدون التطبيق علي ال Production Network تفادياً لحدوث أي مشاكل.

ونأتي للغرض الأساسي من هذا المقال وهو كيفية تطبيق البرنامج علي ال GNS3، ولندع الصور تتكلم:

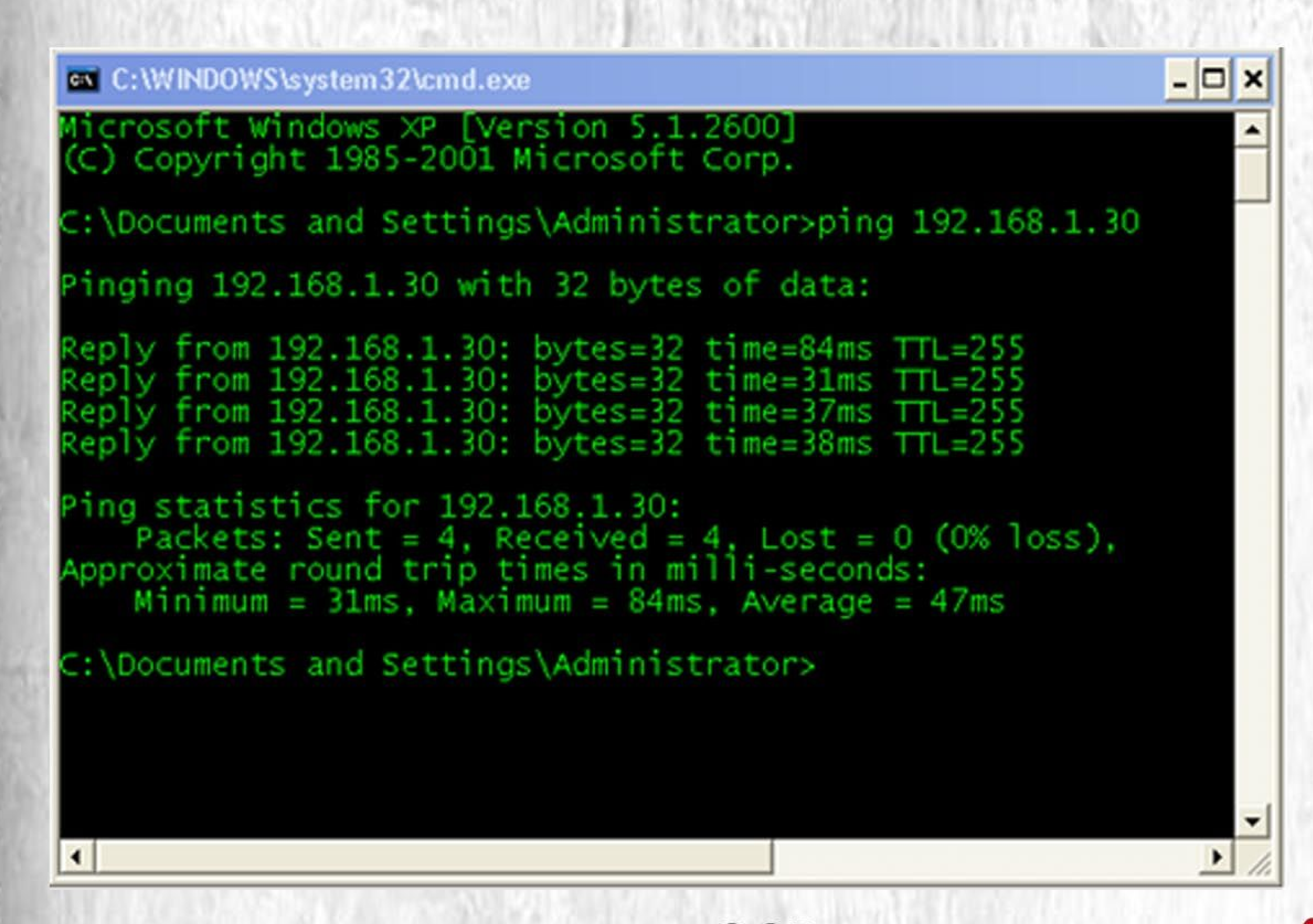
❄1 نقوم بتوصيل الروتر مع الجهاز عن طريق عمل Loopback، أو عن طريق التوصيل مباشرة مع كارت ال NIC



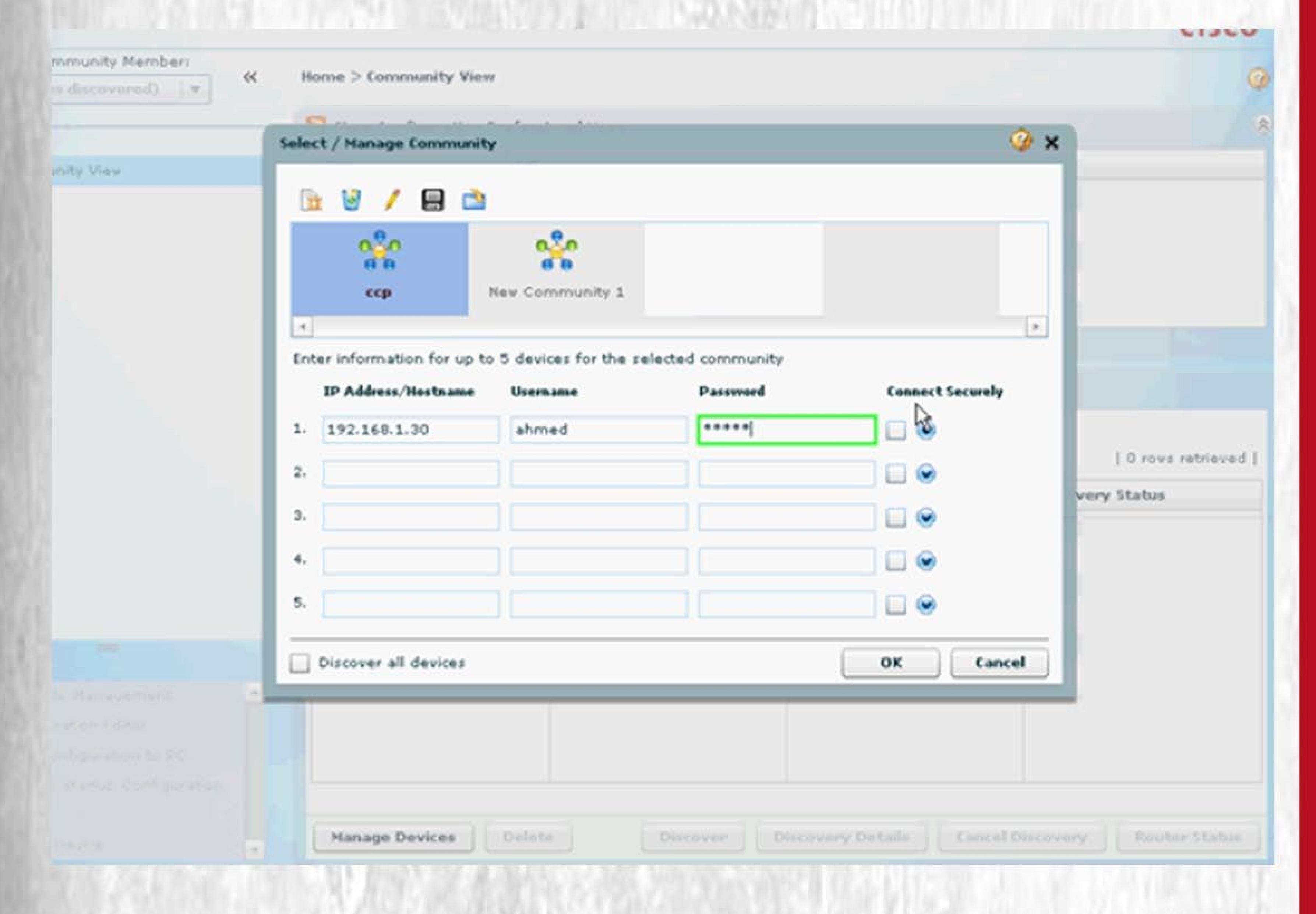
❄2 إعداد الروتر كالآتي:

```
R1#conf t
R1(config)#inter f00/
R1(config-if)#ip add 192.168.1.30
255.255.255.0
R1(config-if)#no sh
R1(config-if)#exit
Enter configuration commands, one per
line.  End with CNTL/Z.
R1(config)#ip http server
R1(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will
be non-exportable...[OK]
R1(config)#
*Mar 11 01:50:57.423: %SSH-5-ENABLED:
SSH 1.99 has been enabled
*Mar 11 01:50:58.743:
%PKI-4-NOAUTOSAVE: Configuration was
modified.  Issue "write memory" to save
new certificate
R1(config)#ip http authentication local
R1(config)#user ahmedprivilige 15 secret
cisco
R1(config)#username ahmed privilege 15
secret cisco
R1(config)#line vty 0 4
R1(config-line)#privilege level 15
R1(config-line)#login local
R1(config-line)#transport input all
```

❄3 نتأكد من أن الروتر قادر على الإتصال بال NIC عن طريق عمل PING



❄4 نقوم بفتح ال CCP وإدخال عنوان الروتر وإسم المستخدم وكلمة السر:



ثم نضغط على Discover ليبدأ البرنامج في إستكشاف الروتر وتجهيزه للعمل.

وفي الختام أسأل الله عز وجل أن ينفعني وإياكم بهذا العلم.



CLEAROS

عبد الجليل الوكيل

أولا أحب أن أشكر الله سبحانه و تعالى، ثم أشكر المجلة و أخص المهندس أيمن النعيمي لإتاحة الفرصة لي للكتابة بهذه المجلة الرائعة التي بدأ إنتشارها في أوساط المنتديات و المدونات العربية بفضل الله سبحانه و تعالى.

و بما أن هذا أول مقال لي في هذه المجلة أحببت أن أبدأ بموضوع يعتبر من المواضيع المهمة و المناسبة لمختلف بيئات العمل سواءاً في الـ Small, Medium, Enterprise أو حتى في الشبكات المنزلية.

سأبدأ حديثي عن أحد البرامج أو الأنظمة المفتوحة المصدرالمبنية على Linux. و بدأ هذا النظام تقريبا منذ عام 2000م، و بدأ إنتشاره بشكل واسع. و كان في بدايته يسمى ClarkConnect، و تم تغيير هذا الإسم في منتصف عام 2009م إلى ClearOS. و يعتبر هذا النظام أحد الأنظمة أو كأحد أفضل التوزيعات على Linux، و قد صمم هذا النظام لإدارة الشبكات و خصيصا ليكون كـ Gateway للشبكة لقوة تحمله و لكونه يتمتع بقائمة واسعة من الخدمات و المميزات بالإضافة إلى واجهة رسومية لسهولة الإعدادات GUI.

أنواع أنظمة ClearOS

تم تقسيم الأنظمة في الـ ClearOS إلى:

Software:وهو عبارة عن الـ Operating System الخاص بالـ ClearOS و يمكن تثبيته على أي جهاز شخصي بمواصفات معينة و ذلك بناءا على عدد المستخدمين، و الجدول أدناه يبين متطلبات الجهاز لتثبيت النظام:

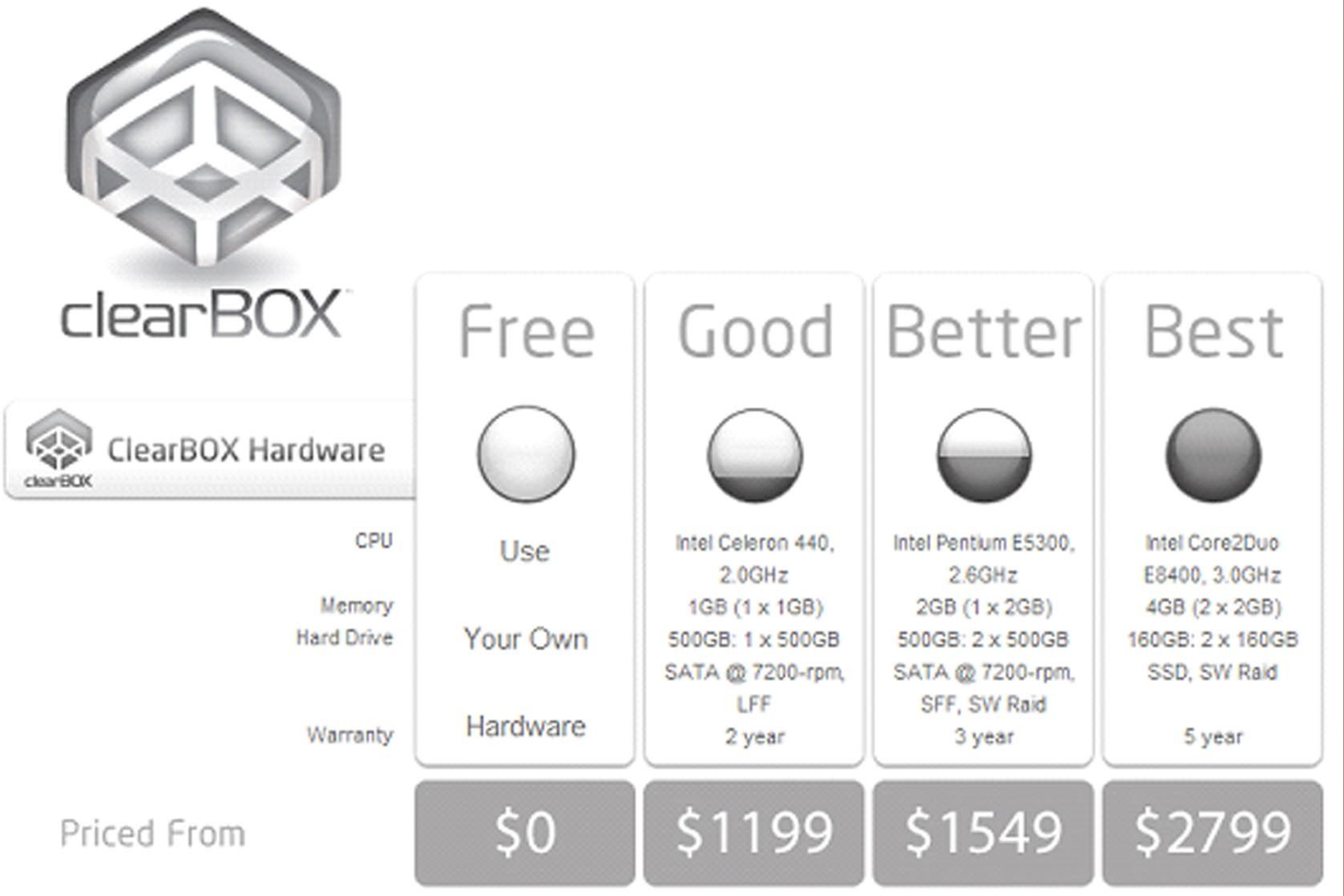
RAM and CPU	5 users	5-10 users	10-50 users	50-200 users
Processor/CPU	500 MHz	1 GHz	2 GHz	3 GHz
Memory/RAM	512 MB	1 GB	1.5 GB	2 GB
Hard Disk				
Hard Disk	Installation and logs require 1 GB - optional storage is up to you			
RAID	Recommended for mission critical systems			

و تم إصدار الـ ClearOS Operating System بأكثر من Version و ذلك بناءا على بيئة العمل و متطلبات العمل. و الجدول أدناه يبين هذه الإصدارات و سعر كل إصدار، والفروق بين هذه الاصدارات

ClearOS Subscription	Free	Good	Better	Best
Subscription Type	ClearOS Basic	ClearOS Basic Plus	ClearOS Standard	Premium
Recommended Environment	Small	Small	Medium	Enterprise
Number of Users	Unlimited	Unlimited	Unlimited	Unlimited
ClearOS Version	5.x	5.x	5.x	5.x
Dynamic DNS	✓	✓	✓	✓
ClearCenter Marketplace Access*	✓	✓	✓	✓
ClearOS Remote Configuration Backup	✓	✓	✓	✓
ClearSDN Services Access*	✓	✓	✓	✓
Dedicated SDN Servers	-	✓	✓	✓
ClearBOX Hardware Access*	-	✓	✓	✓
ClearCARE Support Access*	-	✓	✓	✓
ClearOS Verified Security Updates	-	✓	✓	✓
ClearOS Verified Software Updates	-	-	✓	✓
ClearOS Quality Assurance	-	-	✓	✓
Dynamic VPN	-	-	✓	✓
30-Day Basic Installation Support	-	-	✓	✓
Priority Bug Resolution	-	-	-	✓
Continual Performance Optimization	-	-	-	✓
ClearOS Central Management	-	-	-	Q2-2011
Priced From/Year	$0	$60	$80	$160

و تم إصدار الـ ClearOS Operating System بأكثر من Version و ذلك بناءا على بيئة العمل و متطلبات العمل. و الجدول على اليسار يبين هذه الإصدارات و سعر كل إصدار، والفروق بين هذه الاصدارات

و بعد مشاهدة النوعين من منتجات Clear، راح نتعمق أكثر في معرفة أهم مميزات الـ Software لأنه مناسب تقريبا في أغلب بيئات العمل لرخصه و لإحتوائه على أغلب متطلبات الـ Security



ClearBOX Hardware	Free	Good	Better	Best
CPU	Use	Intel Celeron 440, 2.0GHz	Intel Pentium E5300, 2.6GHz	Intel Core2Duo E8400, 3.0GHz
Memory		1GB (1 x 1GB)	2GB (1 x 2GB)	4GB (2 x 2GB)
Hard Drive	Your Own	500GB: 1 x 500GB SATA @ 7200-rpm, LFF	500GB: 2 x 500GB SATA @ 7200-rpm, SFF, SW Raid	160GB: 2 x 160GB SSD, SW Raid
Warranty	Hardware	2 year	3 year	5 year
Priced From	$0	$1199	$1549	$2799

مميزات النظام (ClearOS Software):

و نظام التشغيل من ClearOS عبارة عن دمج مجموعة كبيرة من البرامج المهمة في إدارة الشبكات غير الخدمات الأساسية. و راح نبدأ بشي من التفصيل لأهم المميزات لهذا النظام:

- Domain Name System DNS: أي بمعنى بإمكانك وضع الـ ClearOS كـ DNS سيرفر الخاص بشبكتك في حال كان لديك Domain.
- Domain Controller DC: بإمكانك عمل مجال أو Domain خاص بشبكتك بدلا عن إستخدام Windows (و هذه الميزات من المميزات الجميلة في هذا البرنامج)، و بكل المميزات التي توجد في Windows Domain مثل الـ Group Policy و الـ ADS و غيرها من مميزات الـ Windows Domain.
- Stateful Firewall: ويعتبر من أقوى أنظمة الجدار الناري لأنه عبارة عن Packet Filtering و يراقب تدفق البيانات من الـ Source إلى الـ Destination بخلاف الـ Stateless Firewall الذي يعتبر بسيط جداً مثل Windows Firewall.
- Load Balancing: و هو عمل موازنة أو إستخدام أكثر من مزود خدمة لموازنة إستخدام الإنترنت، فبإمكانك إستخدام إلى ستة مزودين خدمة (و هذا غير موجود في أي إصدار من إصدارات الـISA أو ال TMG). على سبيل المثال لدي خطين دي إس إل، الأول 2 ميجا والثاني 4 ميجا، وأريد الفئة الذين يستخدمون التصفح وفتح الإيميل أن يستخدموا الخط ال 2 ميجا، أما الذين يستخدمون التحميل والداونلود أن يستخدموا الخط ال 4 ميجا.
- VPN: الشبكات الإفتراضية و التي تمكنك من الولوج أو دخول شبكتك الخاصة من أي مكان عن طريق الإنترنت Virtual Privet Network.
- Bandwidth Management: و هذه ميزة أخرى تفتقر لها منتجات مايكروسوفت مثل الـ ISA أو الـ TMG.
- Demilitarized Zone DMZ: وهو السيرفر أو مجموعة السيرفرات التى يتم وضعها خارج الشبكة الداخلية ليتمكن المستخدم من الدخول عليها من الإنترنت دون إستخدام صلاحيات الشبكة المحلية مثل الـ Username أو ال Password الخاص بالشبكة المحلية.
- Mail Server: و هذه ميزة أخرى، و هي تمكنك من إستخدام الـ ClearOS كـMail Server بدلا من إستخدامك للـ Exchange Server و هذا يفيدك في تقليص التكاليف التي تدفع سنويا لمايكروسوفت كـ License سواءاً لـ Exchange Server نفسه أو للكلاينت CAL .

- Built in Antivirus
- IDS and IPS: و قد تم شرح هذين النظامين في عدد سابق للمجلة (عدد نوفمبر)
- Publishing: يمكنك عمل نشر لموقعك أو سيرفراتك الخاصة عن طريق الـ publishing من خلال نظام الـ ClearOS.
- و غيرها الكثير من الخدمات الأساسية مثل الـ FTP Server, DFS Server, Print Server and Built in MySql.
- بالإضافة إلى الريبورتات التي يمكن الحصول عليها من النظام مثل:

Network Status
Network Traffic
Web proxy report
Resource Reports

و غيرها من الريبورتات التي يمكن الحصول عليها من الـ ClearOS .

متطلبات و كيفية إعداد الـ Operating System:

متطلبات النظام هو كما أسلفنا سابقا بالجدول المبين أعلاه و المتطلبات بناءا على بيئة العمل و عدد المستخدمين و يفضل عمل ال RAID لحماية و تأمين السيرفر من الأعطال المفاجئة و عمل الـ Backup.

و بخصوص كرت الشبكة أو الـ NIC ، فيفضل تركيب كرتين شبكة إذا تم إستخدامه كـGateway ، أو كرت شبكة واحد في حال إستخدام الجهاز كـ Web Cashing.

و ال System يتضمن تعريفات لجميع أنواع كروت الشبكة، ماعادا الWireless NIC فيفضل إستخدام كرت شبكة عادي Fast or Giga Ethernet ، و أيضا إمكانية عمل إعدادات الـ PPOE بمعني عمل إعدادات الـ DSL من البرنامج نفسه بدلا من إستخدام المودم.

و أود التنويه أن هناك بعض الـServices تحتاج إلى معالج قوي و ذاكرة إضافية مثل:

- Intrusion Detection and Prevention
- Content Filtering
- Webmail
- Antispam
- Antivirus

إعدادات و تحميل البرنامج:

بالضغط على الرابط التالى ISO يمكنك تحميل ملف الـ:
http://download.clearfoundation.com/clearos/enterprise/5.2/iso/clearos-enterprise-5.2-service-pack-1.iso

(حجمه 700 ميغا) و طبعا هناك إصدارين 5,1 و 5,2 و يفضل تحميل الإصدار الأخير لإحتواؤه بعض المميزات الجديدة عن الإصدار القديم و الرابط الموجود في الشرح للإصدار الجديد.

طبعا هناك طريقتين لإقلاع البرناج أو الـ Booting :

1* عن طريق الـ CD : و يتم بعمل عمل حرق أو burn لملف الـ ISO على الـ CD.

2* الثانية عن طريق Bootable USB : ويمكنك تحميل البرنامج بالضغط على الرابط التالى:
http://download.clearfoundation.com/clearos/enterprise/5.2/images/diskboot.img
(لعمل الـ Bootable USB)

و تثبيت البرنامج سهل جداً، و يمكنكم مشاهدة الفيديو الخاص بكيفية تثبيت البرنامج من الرابط التالي:
http://jallooo.wordpress.com/2011/02/24/clear-os-نظام-تشغيل-مجاني

و من الأشياء الجميلة التي قدمتها الشركة المنتجة لهذا البرنامج هو عمل Online Demo لمعرفة مميزات البرنامج و الخدمات التي يشملها البرنامج و يمكنك مشاهدة الـDemo بالضغط على الرابط التالى:
https://demo1.clearos.com:81/admin/users.php

إسم المستخدم هو get و كلمة المرور هى clear .

و لمزيد من المعلومات يمكنك الإطلاع على البرنامج من الموقع الرسمي
http://www.clearfoundation.com



Integratoin Technical Solution

Network - Web Design

Training & Development

Programing - Design & Printing

Electronic System - Control System

Whole Technical
One Supplire

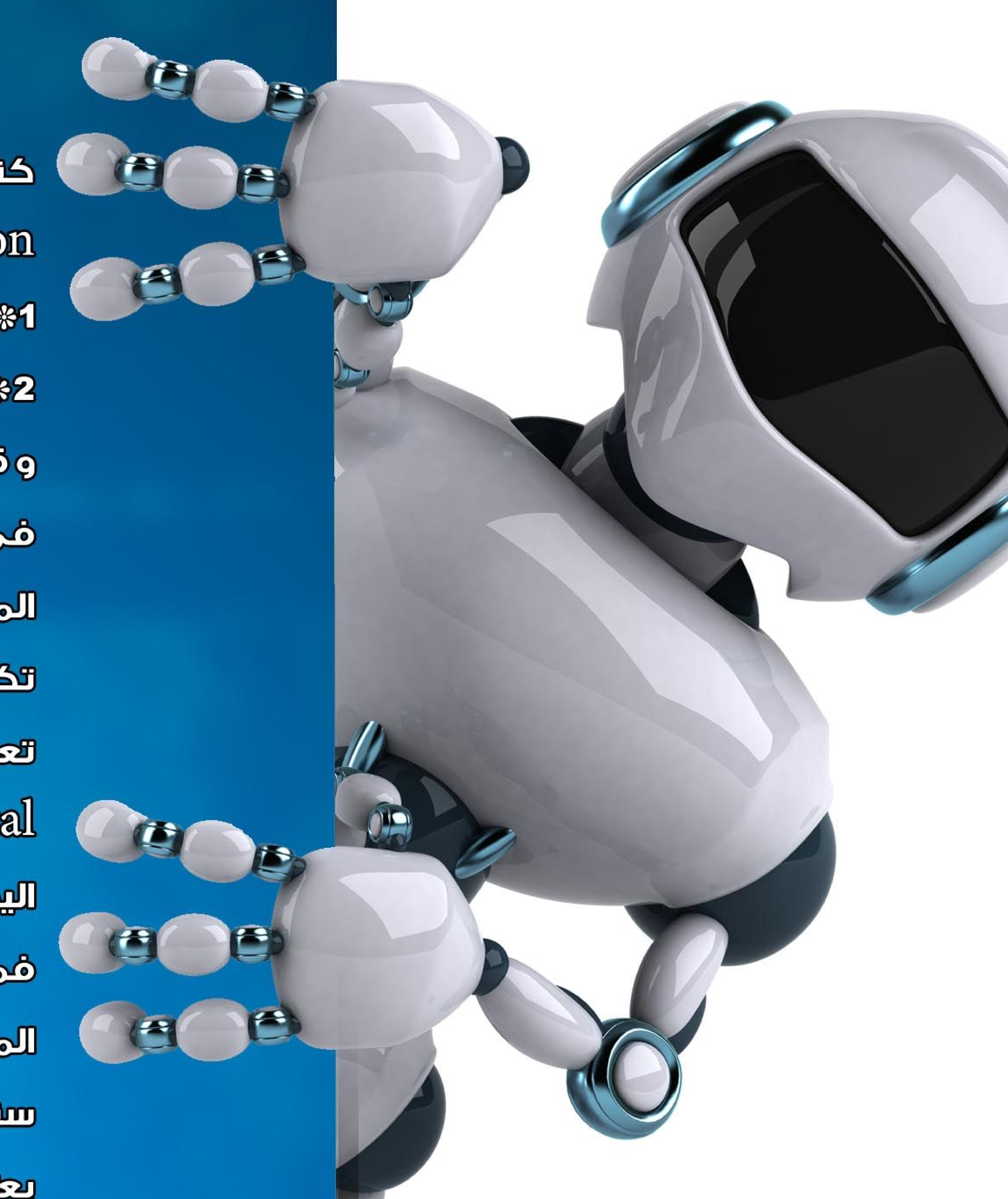
Study and implementation of engineering projects

Syria - DeirEzzor - Telefax: 051 218452 - Mob: 0967 96265 - 0955 478942
Website:WWW.EchoTechno.com - E-mail:Info@EchoTechno.com (Soon)

الفرق بين ال ESX وال ESXi

الحلقة الثانية من تقنية VMWARE مع ال Virtualisation

عبد الرحمن بن داود



كنا قد تكلمنا في الموضوع السابق عن أنواع ال Virtualization والتي هي نوعين:

1* Bare-Metal

2* Host-Based

و قلنا أن النوع الأول (أى ال Bare-Metal) هو الذي يهمنا في سلسلة شروحاتنا لمنتجات VMware، لأنه الحل المخصص للشركات ذات أنظمة المعلومات الضخمة (حيث تكثر فيها السيرفرات).

تعرض VMware منتجين أساسيين تحت مظلة ال Bare-Metal وهما ال ESX وال ESXi أو ما أصبح يعرف اليوم بال vSphere.

فما الفرق بينهما ؟ وأي واحد يختاره المسؤول عن نظام المعلومات؟ وأي منهما يمثل الحل الأنسب لشركتي ؟ هذا ما سنجيب عنه في هذا الموضوع المختصر.

يعتبر ال ESX الحل القديم والأكثر متانة إذا ما قورن بال ESXi الذي أثبت خفته و أمنه العالي، ولكن إذا لاحظنا التطور الحاصل فإننا سنجزم بأن أيامه معدودة، و هذا ما صرحت به شركة VMware ، فنهاية 2011 ستكون نهاية ال ESX و لذلك تعمدت الشركة إصدار النسختين معا لمدة تزيد عن السنتين حتى يتسنى للشركات ترقية ال ESX إلى ESXi أي عمل (upgrade).

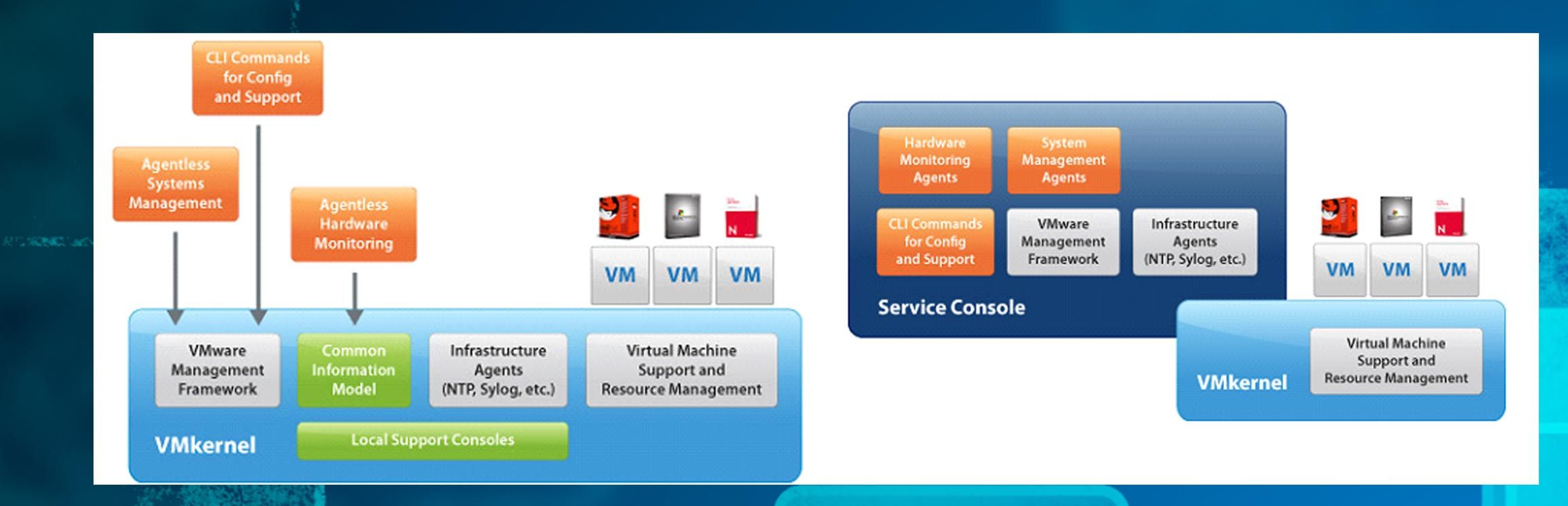
يمكن إحصاء الكثير من الاختلافات بين الإصدارين إلا أنه يمكن حصرها فيما يلي علما بأن أغلبها تقنية :

1- أول اختلاف بينهما وهو الإختلاف الأساسي : يكمن في الهندسة أو التصميم. فال ESX يعتمد على ما يسمى بال Service console وهي عبارة عن نظام تشغيل إفتراضي (RedHat Virtual Machine)، يتم تسطيبه تلقائيا مع عملية التنصيب الأولية لل ESX ويتم من خلاله التعامل مع ال VMKernel (الذي يربط بين ال Hardware وال VMs) وإدارته و التحكم فيه.

تستعمل أيضا ال SC للربط بين ال VMKernel والتطبيقات (البرامج) التي توفرها شركات أخرى وبالخصوص برامج المراقبة (Monitoring) والحماية (Security).

أما على مستوى ال ESXi فقد تم حذف ال SC ولذلك يلاحظ فرق كبير بينهما من حيث سرعة التحميل (Loading)، و إستعمال أقل للهاردوير(Performance).

و إليكما مخططان يسهلان فهم الفرق بين الإشتغال بوجود ال Service Console(SC) و في غيابها:



إلا أنه يمكن التعامل مع ال ESXi في البداية من خلال واجهة تمكننا من تعيين كلمة السر لل root و كذلك المعلومات المبدئية للشبكة كال ip address و الdefault gateway و الDNS ، و هي ما يسمى بالDirect Console User Interface(DCUI) وهذه صورة توضح شكلها.



لو قارنا حجم القرص الذي يشغله ال ESX لوجدنا أنه على الأقل يأخذ2GB (لوجود ال SCعلى هيئة Virtual Machine لا تظهر)، أما ال ESXi فيتطلب 32Mb وهذا ما يسهل عملية تنصيبه (SD flash or USB key تكفي).

هناك طريقة وحيدة لتنصيب و إقلاع الESX وهي عن طريق الCD/DVD أو باستعمال الإقلاع عن طريق شبكة تخزين مركزية (SAN). أما ال ESXiفزيادة على ذلك يمكن أن يشترى شبه منصب في الهاردوير بإستعمال رقائق فلاش وهذا يتم على مستوى الشركات المتعاقدة مع VMware مثل DELL وهو ما يسمى بال EMBEDDEDوما يسهل هذه العملية هو صغر الحجم الذي يستهلكه الESXi مقارنة بال ESX.

يتميز الESXi بسرعة الإقلاع وإستغلال جيد للهاردوير مقارنة بالESX فمثلا ال SC يمكنها أن تصل إلى 800Mb إستهلاك من الRAM، في حين أن هذا تم اجتنابه مع ال ESXi.

بما أن ال ESX يحتوي على إصدار RedHat(SC) فهو لا يتطلب فقط التحديثات والتصحيحات (updates and patches) الخاصة فقط بال VMKernel، بل يبحث عن تحديثات وتصحيحات الService Console أيضا، أما ال ESXi فيختزل كل هذا في ال VMKernel فقط.

كل هذا يساعد على ضمان الإستقرار للنظام لأنه معلوم أن مع كل تحديث أو تصحيح يجب إعادة تشغيل النظام، فال ESXi يضمن إستقرار أفضل من ال ESX.

يعتبر ال ESXi أأمن من ال ESX، لأن معظم البورتات و الخدمات موقفة تلقائيا، عكس الثاني الذي يتحتم عليه فتح بعض البورتات للتوفيق بين عمل ال VMKernel و ال SC.

أما بخصوص إدارة ال ESXi فهو يفتقر لل Console التي إعتاد مستخدمو ال ESX إدارته من خلالها ولذلك يمكن حصر إدارة المنتجين كما يلي:

ESX Management :

- ❋ vCenter Server.
- ❋ vSphere Client.
- ❋ Built-in Web Service.
- ❋ CLI (SSH) to Console.

ESXi Management :

- ❋ vCenter Server (for licenced ESXi)
- ❋ vSphere Client (for free ESXi)
- ❋vCLI and PowerCLI vMA (من أجل إصدار أوامر عن بعدremote execution of scripts and commands)

إعلم أخي أنه يمكنك إستعمال ال ESXi بدون مقابل، و هذا غير موجود مع ال ESX مع محدودية طبعا، و من جملة ذلك أن الvCLI و الPowerCLI سيكون read only علما أنه لا يمكن استخدام ال SNMP، و لا يمكن إستخدام عدد كبير من الخواص التي تميز VMware عن باقي المنتجين و الجدول الآتي يوضح ما أنا بصدد قوله:

	ESXi – Free License (ESX not available without VI)	VI Foundation (with ESX or ESXi)	VI Standard (with ESX or ESXi)	VI Enterprise (with ESX or ESXi)
Core hypervisor functionality	Yes	Yes	Yes	Yes
Virtual SMP	Yes	Yes	Yes	Yes
VMFS	Yes	Yes	Yes	Yes
VirtualCenter Agent		Yes	Yes	Yes
Update Manager		Yes	Yes	Yes
Consolidated Backup		Yes	Yes	Yes
High Availability			Yes	Yes
VMotion				Yes
Storage VMotion				Yes
DRS				Yes
DPM				Yes

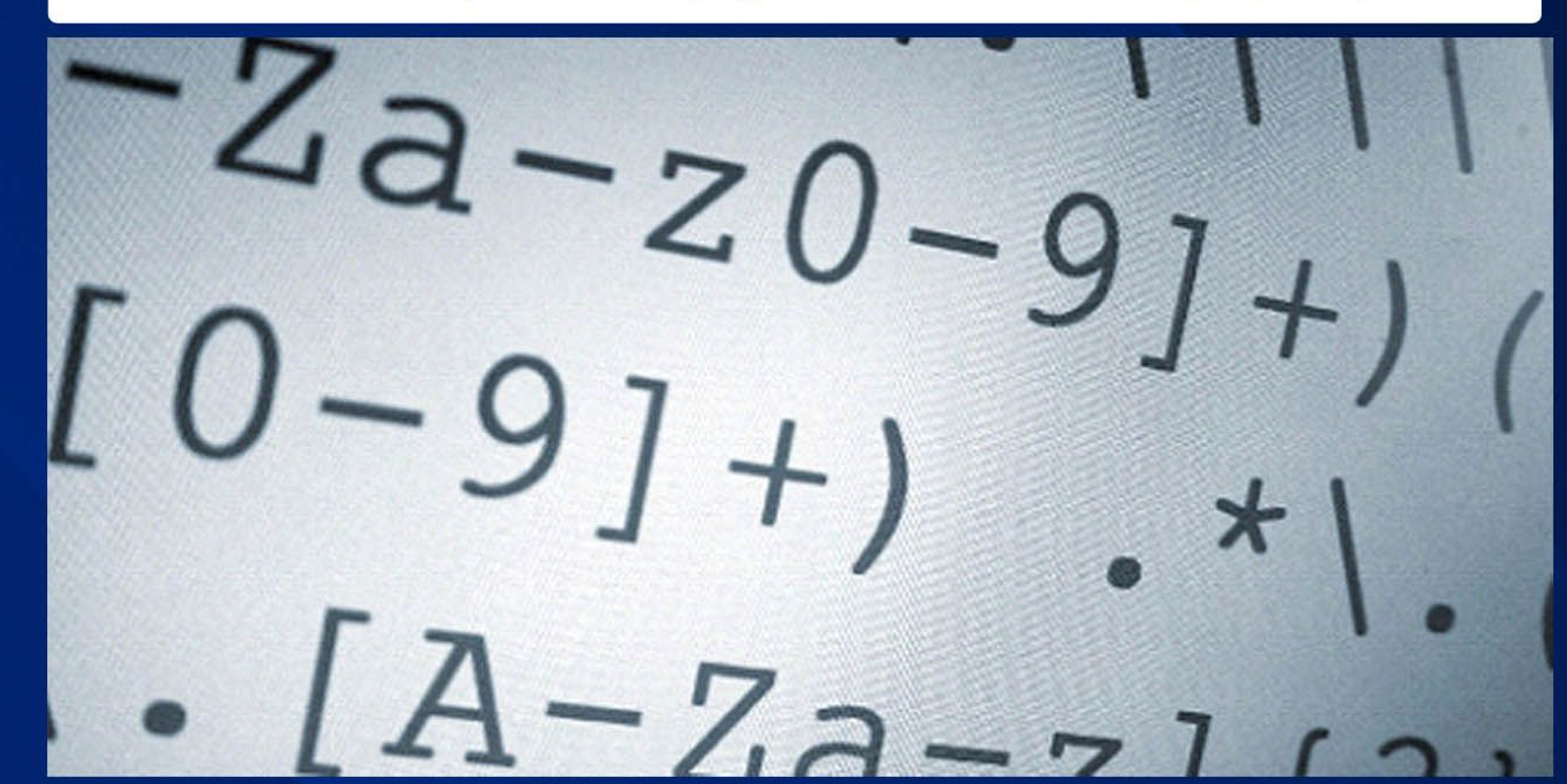
هناك إختلاف أيضا في الصيانة فال ESX تتم صيانته عن طريق ال SC أما ال ESXi فعن طريق الPowerCLI أو الvCLI أما الصيانة المتقدمة فتتم بواسطة Tech Support Mode الذي يمكن الدخول عليه بطريقتين:

❋ إما الدخول على الواجهة المباشرة المتاحة تلقائياDCUI

❋ أو ال SSH

تنبيه: هنا تجدر الإشارة أنه يتم الدخول على الواجهة DCUI التي تتعامل مباشرة مع ال VMKernel من دون وجود وسيط كما في حالة ال ESX و هو SC. و في الأخير أود أن ألخص ما سبق ذكره، و التنويه بأن أكبر فرق بين الإصدارين هو ال Service Console، و هذا الذي يجب تذكره. أما باقي الفروق فتبقى سطحية و لا يتسع المجال لذكرها كلها لأن الهدف من هذا الموضوع هو إعطاء نبذة عن ال ESX و ال ESXi. أما فيما يتعلق بالإختيار بينهما فالأولى بالمهتم بهذه التقنية مراجعة متطلبات نظامه، فإن كان يعتمد على تطبيقات و برامج سيتم إدماجها مع ال VMware فالأفضل إستعمال الESX كاملا، أما من أراد الحصول على تقنية الvirtualization و كفى فليستعمل ال ESXi الذي يعتبر أرخص من الناحية المادية و أسرع و أأمن من سابقه.

(REGEX)Regular Expression
ودورها فى تأمين الشبكه



مقدمة :

إستكمالا للموضوع السابق حول أجهزة ال IPS & IDS تطرقت إلى موضوع ال regular expression هذا ولكن لم أتكلم عنه بالتفصيل، مما دفعنى إلى تخصيص مقال لهذا الموضوع، فالكثيرلايعلم شىء حول هذا الموضوع بالرغم من أن له بعض التطبيقات فى أجهزة Cisco المختلفه سواء كانت IPS & IDS OR ASA firewall OR Router، وإن كان يستخدم كثيرا جدا فى البرمجه ومن لديه خلفيه برمجيه سيجد الموضوع بسيط جدا.

تعريف ال Regular Expression :

تبسيطا لفكره ال Regular Expression سأستعين بمثال بسيط لشرح الفكرة:

مثال 1 : لدينا شبكه يوجد بها FTP server غايه فى الأهميه، وتأمينا له وضعناه خلف جهاز IPS sensor ليقوم بفحص ال Traffic المرسله إليه، فى أحد الأيام تم إكتشاف ثغره تستهدف ال FTP servers، الأن يجب علينا أن نقوم بتأمين ال server لدينا، ولكن كيف؟؟ Cisco لم تطرح بعد أى signature تقوم بكشف الهجوم، إذن لايوجد أمامنا الأن إلا تصميم signature لهذاالهجوم.

أولا قمنا بعمل بحث حول هذا الهجوم ووجدنا الأتى - هذا الهجوم يحتوى على هذه ال string التى تقوم بتنفيذ شىء خبيث فى ال server ولتكن هذه الكلمه هى ATTACK، الأن قمنا بعمل ال configuration اللازم لل IPS ليقوم بكشف الهجوم والذى يتعرف عليه عن طريق البحث داخل ال packetعن الكلمه ATTACK، ولكن هل هذا كافى؟

تابعوا معى لتعرفوا أن ال HACKER الذكى لايعتمد على طريقة واحدة فى تنفيذ هجوم ما، بل يقوم بتغير طريقته ليتفادى الكشف، فإذا قام مخترق بمحاوله تنفيذ هجوم على ال FTP server الذى نتولى عمليه تأمينه الأن، و تفاجأ هذا المخترق بأن الهجوم لم ينجح، لذلك فسوف يفكر فى طريقه لخداع جهاز ال IPS الذى يؤمن شبكتنا، فمن الممكن أن يقوم هذا الشخص بتعديل بسيط فى الهجوم وهو كالأتى، فبدلا من أن يحتوى الهجوم على كلمه ATTACK قام بتغييرهذه ال string إلى ATTacK، مجرد تغيير حرفين من CASE إلى LOWER-CASE ولكن النتيجه قد لا تسرنا، أولا عندما مرهذا الهجوم على ال ips قام هذا الأخير بعرضه على مجموعه من ال signatures التى تقوم بفحص البيانات ومن بينها ال sig التى قمنا بتصميمها، عندما بدأت هذه ال sig فحص الهجوم لم تكتشفه لأنها تعتمدعلى شكل واحد للكلمة ATTACK الموجودة فى الهجوم للتعرف عليه، والأن هذا الهجوم تجاوز ال IPS، ووصل إلى ال server ونجح فى تنفيذ أعمال تخريبيه فى ال server.

الأن ما الحل لمثل هذه المشكله؟ أسمع من يقول بذكاء "بسيطة يمكننا أن نقوم بعمل sig أخرى لتقوم بمنع أى packet تحتوى على أى string من الأتى ATTACK أو ATTack أو ATTack أو attack أو attack إلخ ...

ممتازولكن ماهى الطريقة التى نستطيع بها تحديد أى شكل ما لهذه الكلمه؟ غيرمعقول طبعا أن نصمم signature واحده لكل شكل من هذه الكلمه، فمثلا sig 1 تقوم بكشف attack و2 sig تقوم بكشف ATTAck إلخ ...

طبعا هذا مستحيل لأنه فى الهجوم الحقيقى لن تكون مجرد كلمه من ستة أحرف فقط ! هنا يأتى دور Regular Expression لتساعدنا فى تحديد هذه الكلمه بأى شكل لها، فال Regular Expression عبارة عن notational language أو لغه ترميزية تساعدنا لعمل وصف ل text pattern، فمثلا لنقوم بعمل وصف للكلمة ATTACK بكل أشكالها بمساعده ال regular expression سنفعل الأتى "(Aa)(Tt)(Aa)(Cc)(Kk)" هل رأيتم السهوله التى إستطعنا بها عمل match للكلمه بكل أشكالها

الأن نضع هذا النص "(Aa)(Tt)(Aa)(Cc)(Kk)" فى ال signature وستقوم ال signature بمنع أى packet تحتوى على أى شكل من هذه الكلمه.

تستخدم ال regular expression مجموعه من الرموز تسمى Metacharacters تعطى مرونه لوصف أى نص نريده ، فمثلا إستخدمنا هذه الاقواس ( ) وهى تدل على كلمه attack بجميع أشكالها عن طريق إستخدام حرف واحد من كل قوس، نأخذ مثال أخر لنفهم اكثر

نريد ال regular expression التى تمثل الكلمتين hacker أو Hacker الحل هو (Hh)acker

نريد ال regular expression التى تمثل الكلمتين hacker أو Hacker الحل هو (Hh)ack(Ee)r

نريد ال regular expression التى تمثل الكلمتين hat أو hot الحل هو h(oa)t

أعتقد أن الأمر أصبح واضحا الأن ، ولكن هناك رموز أخرى كثيرة تساعدنا فى هذه العمليه تعالوا نتعرف على أهمها

ال Regular Expression Metacharacters :

Symbol	Meaning
?	Repeat 0 or 1 times
*	Repeat 0 or more times
+	Repeat 1 or more times
{x}	Repeat exactly X times
.	Any one character except \n or \t
[abc]	Any character listed
[^abc]	Any character not listed
[a-z]	Any character listed inclusively in range
()	Used to limit the scope of other metacharacters
^	The position at the start of the line
\char	Literal character match, including metacharacters
char	Matches character literally, not including metacharacters
|	OR of two regular expressions
\n	Line feed
\t	Tab

networkset

علامة الإستفهام ?

تعنى هذه العلامة إحتماليه وجود الحرف الذى يسبقها أو قد لا يوجد

مثال – he?llo تقوم بعمل match لـ hello أو hllo

مثال – pl?ay تقوم بعمل match لـ play أو pay

النجمه * asterisk

تعنى إحتماليه تكرار الحرف الذى يسبقها أكثرمن مرة أو قد لا يوجد نهائيا

مثال – lo?se تقوم بعمل match لـ lse أو lose أو loose أو loose أو looooooose أوإلخ ...

علامه +

تعنى إحتماليه تكرارالحرف الذى يسبقها أكثر من مرة أو على الأقل وجوده مرة واحده

مثال – lo+se تقوم بعمل match لـ lose أو loose أو loose أو looooooose أو إلخ .. (لاتقوم بعمل match ل lse لأنها تشترط وجود الحرف مرة واحده على الأقل)

زوج الاقواس {}

يستخدم هذا النوع لتحديد عدد تكرار حرف معين، و ذلك بإدخال رقم داخله ، وهذا الرقم يشير إلى عدد مرات التكرار للحرف الذى يسبق القوس

مثال – l{3}ose تقوم بعمل match لـ lllose

زوج الاقواس ()

يقوم بتجميع عدد من الأحرف بداخله ليتم معاملتهم كأنهم حرف واحد فقط

مثال - {4}(xyz) تقوم بعمل match لـ xyzxyzxyzxyz (تم معاملتها داخل الأقواس كأنه كيان واحد)

النقطة .

تشير النقطة إلى أنه من الممكن أن يكون مكانها أى حرف فيتم تجاهل أى شيء مكانها

مثال - h.t تقوم بعمل match لـ hat أو hot أو hit أو إلخ ....

زوج الاقواس [ ]

تحديد عدد من الخيارات المتوقعه بداخله

مثال - (Aa) تقوم بعمل match ل A أو a

مثال - (Hh)(Ee)(Ll)(Ll)(Oo) تقوم بعمل match لكلمه hello بجميع حالاتها سواء كانت capital or small

العلامه ^

مع زوج الاقواس ( ) - تساوى هذه العلامه كلمه NOT

مثال - (^abc) تقوم بعمل match لأى حرف غير a أو b أو c

العلامه ^ منفرده

تستخدم إذا أردنا عمل match لجملة أو أى text يبدأ بكلمه معينه

مثال - ^hello تقوم بعمل match لأى سطر يبدأ بكلمه hello مثل hello sherif أو hello ali أو hello .... إلخ

علامه $

تستخدم إذا أردنا عمل match لجمله أو أى نص ينتهى بكلمة معينة

مثال - xyz$ تقوم بعمل match لأى سطر ينتهى ب xyz مثل aaaaaxyz أو ggggxyz إلخ ..

الشرطة "-"

تقوم بتحديد range معين

مثال - بدلا من كتابة (abcdef) يمكننا كتابه (a-f) تقوم بعمل match لأى حرف فى هذا ال range

مثال - (1-9) تقوم بعمل match لأى رقم فى هذا ال range

علامه |

هذه العلامة تساوى كلمة OR

مثال - (sherif)|(magdy) تقوم بعمل match لكلمة sherif أو magdy (لاحظ إستخدام الأقواس)

مثال - (a-f)|(G-Z) تقوم بعمل match لأى حرف small من a إلى f أو حرف capital من G إلى Z (لاحظ الفرق بين هذا النوع من الأقواس والنوع السابق)

العلامة \

هذه لها مدلول مختلف فهى تسمى "escape character"، حتى أستطيع شرح هذه العلامة تابعواهذا المثال

مثال - نريد أن تقوم بعمل match ل IP address معين لنفترض مثلا 192.168.10.10 ، المشكله هنا هو أن هذا string يحتوى على علامة مميزة بالنسبه لل REG EXP وهى النقطة

لذلك لكى نزيل معنى هذه النقطة ونجعلها مثل أى حرف أخر نفعل الأتى 192\.168\.10\.10 حيث قامت الـ \ بجعل النقطة مثل أى حرف أخر ، ويمكننا إستخدام هذه العلامة مع أى metacharacter أخرى لعمل match لأى نص يحتوى على أحد هذه العلامات.

مثال مفصل :

الأن سأقوم بشرح REGEX تقوم بعمل match لأى E-mail للتحكم بمدخلات المستخدم

9a-z_)+ @(Nn)(Ee)(Tt)(Ww)(Oo)(-A-Z0
(Rr)(Ss)(Ee)(Tt)\.(com)|(net

نبدأ بالجزء الأول من الـ REGEX

+ (_9a-z-A-Z0)

الأقواس من النوع () تخبرنا أنه يمكن إختيار أى شيء من داخلها مثلا

أى حرف من ال range الأول و هو من A الى Z (Upper-case)

أو

أى رقم من ال range الثانى و هو من 0 إلى 9

أو

أى حرف من ال range الثالث و هو من a إلى z (Lower-case)

أو

علامة الـ _

بعد ذلك تأتى علامة الـ + تقول لنا أنه يمكننا تكرار ما سبق على الأقل وجوده مرة واحدة أو أكثر وذلك لمنع

المستخدم من ترك هذا الجزء فارغ

بعد ذلك يجب وجود علامة @ ثم كلمه networkset بجميع حالاتها ثم النقطة بعد ذلك وتم إستخدام الـ \ ليتم معاملة النقطة كأنها حرف عادى.

أخيرا نترك خيارين فى النهايه وهو أن ينتهى بـ com أو net بإستخدام | التى تساوى OR

تطبيقات ال Regular Expression فى أجهزة Cisco

يوجد العديد من التطبيقات على أجهزة cisco يستخدم فيها ال Regular Expression وسأحاول تلخيص أهمها الأن:

أولا: cisco router تستخدم ال Regular Expression فى ال BGP ومن يدرس شهاده CCIE R & S أعتقد أن يعرف هذا الموضوع ويجب أن يكون ملم بال Regular Expression جيدا.

ثانيا: ASA Firewall تستخدم الـ Regular Expression فى الـ MPF(Modular Policy Framework) أو مايسمى ب MQC إذا تم تطبيقه على Router.

ثالثا: IPS & IDS راجع مثال 1

رابعا: فى الأمر show run على أى جهاز cisco شاهد

مثال 2 : أثناء القيام ب troubleshooting or verifying للإعدادات أو ال configuration على router أو switch أو firewall نحتاج إلى تحديد مخرجات معينة للتركيز عليها، فبدلا من مشاهدة ملف ال configuration كاملا، يمكننا تحديد جزء معين لنراه

```
NetworkSet#show running-config | include ?
  LINE  Regular Expression

NetworkSet#show running-config | include h[ao]t
username hot
username hat
NetworkSet#
```

وكما نرى يمكننا إستخدام Regular Expression لتحديد مخرجات معينه، وهذا مثال أخر:

```
NetworkSet#show running-config | include magdy$
username sherif-magdy
NetworkSet#
```

أتركـكم لتجربوا هذه الطريقة بأنفسكم ، فهى تسهل العمل إذا كان ال configuration file كبيرالحجم.

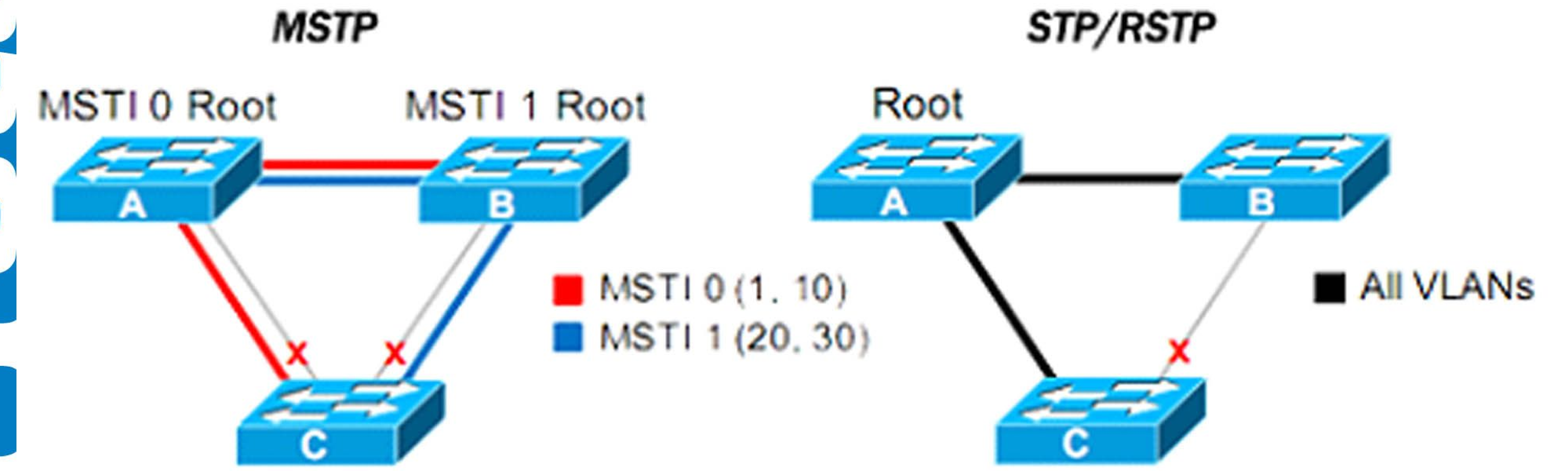
خاتمة :

هذه مجرد نظرة موجزة للموضوع فهو له تطبيقات كثيرة فى غاية التعقيد، و أجد بعض التشابه بينه و بين ال subneting عندما بدأت تدرسه فى ccna و كنت ترى أنه معقد و صعب الفهم و لكن بعد فهمه جيدا تجده فى منتهى السهولة، هذا هو الحال مع الـ Regular expression و هناك الكثير من الكتب تشرحه بالتفصيل .

شريف مجدي



IEEE

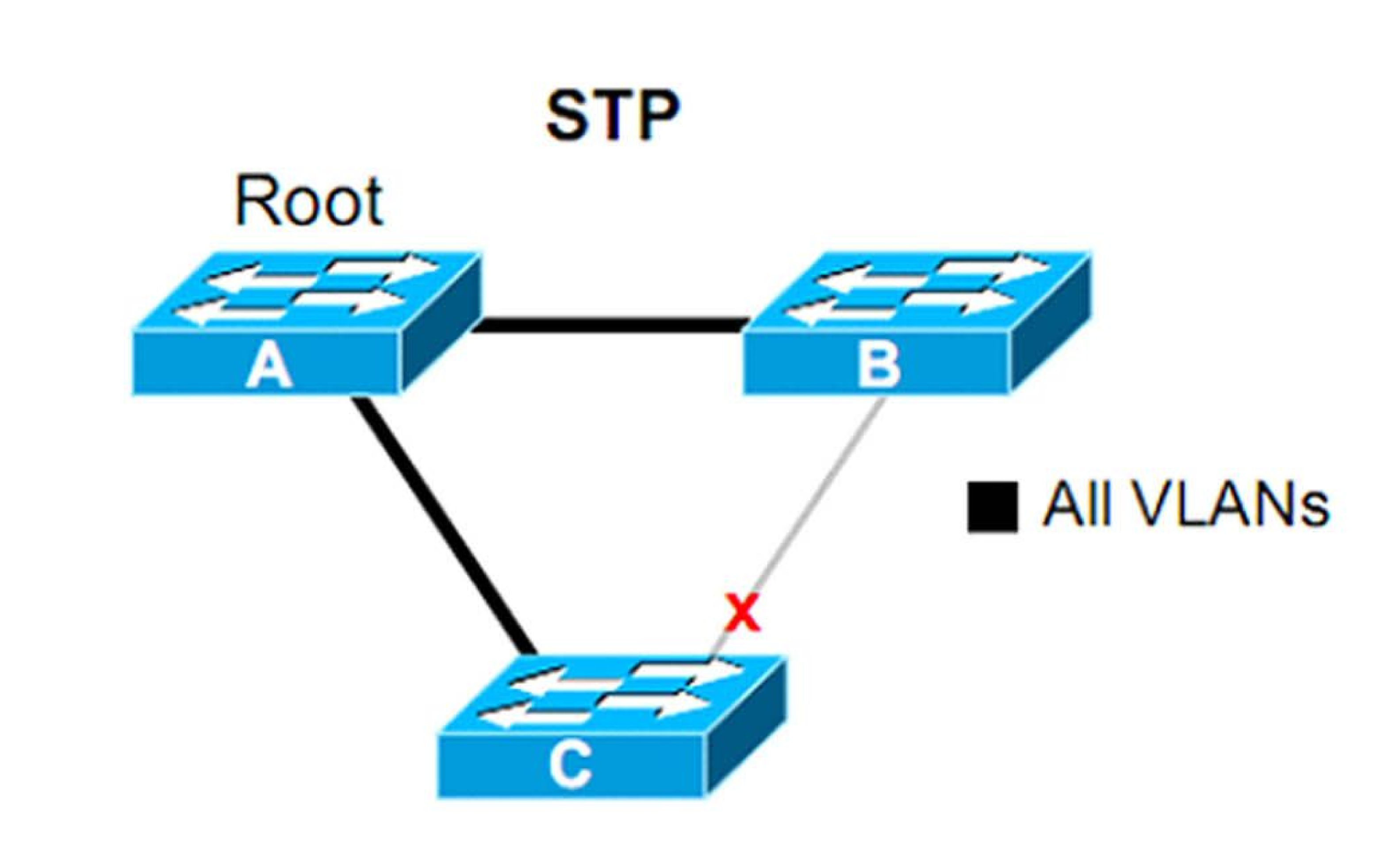


أغلبنا وإن لم يكن جميعنا قد مر أثناء دراسته على بروتوكول الـ STP وعلى الأغلب أن هناك من وجد صعوبات وتعقيدات كثيرة في أنواعه المتوفرة فمن خلال إحصائية صغيرة قمت بها أحصيت على الأقل ستة أنواع لهذا البروتوكول وهي CST, RSTP, MSTP, PVST, RPVST , PVST+.

لنتعرف اليوم في القسم الأول من هذا المقال على أهم الإختلافات الموجودة بين STP, RSTP, MSTP والخاصة بي IEEE. وقبل أن أبدا أحب أن أنوه أن هذه البروتوكولات لها وظيفة واحدة وهي منع حدوث مايعرف ب اللوب (Loop) على مستوى الطبقة الثانية Data Link .

بالإضافة إلى أن الموضوع لن يكون حول ألية عمل كل واحد منها لأنها بحسب إعتقادي معروفة عند الجميع، بل فقط عن الأختلافات بينها ولنبدأ ب البروتوكولات الخاصة ب IEEE:

CST: أو Common Spanning Tree أو الـSTP الذي نسمع عنه والذي يعرف من خلال منظمة IEEE ب 802.1D يتصف هذا البروتوكول بأنه يعمل على كل أنواع الأجهزة سيسكو كانت أم جونيبر وبدون تفريق. ومايميزه هو وجود نسخةSpanning Tree واحدة أو One Instance تضم جميع الـ Vlans ويتم تبادل ال BPDU بين السويتشات من خلال ال Native Vlan، وهو يعمل من خلال Instance واحدة تضم كل البورتات وتضم كل الـ Vlans الموجودة في الشبكة (سوف نفهم فكرة الـ Instance أكثر عندما نصل إلى MSTP) وهذه صورة توضيحية لل CST .



Protocol وهو نموذج مطور من STP ويعرف ب 802.1W ومن خلال إسمه نستطيع أن نستنتج أن هذا البروتوكول هو أسرع من البروتوكول العادي والأسباب كثيرة:

✻1 تم دمج حالتا الـ Blocking و Listening إلى حالة واحدة وهي ال Discarding وكما هو معروف أن الوصول إلى حالة ال Listening كان يستغرق 15 ثانية .

✻2 الزمن الذي يلزم لإنتقال البورت من Dis-carding إلى Learning هو 6 ثواني، وهي تعني عدم إستلام BPDU ل 3 مرات متعاقبة لأن الـBPDU ترسل كل ثانيتين وهذا يعطينا 6 ثواني فقط، بينما نجد أن ال STP يحتاج منك 20 ثانية للدخول في مرحلة ال Listening، أي يجب أن ينتظر البروتوكول توقف إستلام ال BPDU لعشر مرات.

(فكرة الإنتقال تعتمد على عدد مرات إستلام الـ BPDU وليس على زمن معين، أى أن البروتوكول يحسب عدد مرات عدم إستلام ال BPDU، ونستطيع نحن من خلال ذلك أن نستنتج الوقت اللازم).

✻3 من خلال هذه المقارنة نجد أن الـSTP يستغرق حوالي 50 ثانية لكي يتحول من حالة الـ Block إلى حالة الـForward بينما الـ RSTP يستغرق حوالي 21 ثانية.

✻4 تسميتان جديدتان حلتا مكان Blocking Port وهي Alternate Port & Backup Port الأول هو بورت إحتياطي لكل segment موجودة في الشبكة، والثاني هو بورت بديل للـ Root Port.

✻5 في الـSTP كان الروت بريدج هو الوحيد الذي يقوم بإرسال BPDU، وبعدها تتناوب باقى السويتشات على الإرسال. أما مع الـRSTP فكل السويتشات الموجودة يمكنها أن تقوم بإرسال BPDU، فلو كان لدينا سويتشان موجودان ضمن شبكة كبيرة وأصبح أحد البورتات فى حالة Down، فإن السويتش سوف يرسل BPDU إلى السويتش الأخر لكي يقوم بتفعيل البورت الإحتياطي بشكل مباشر.

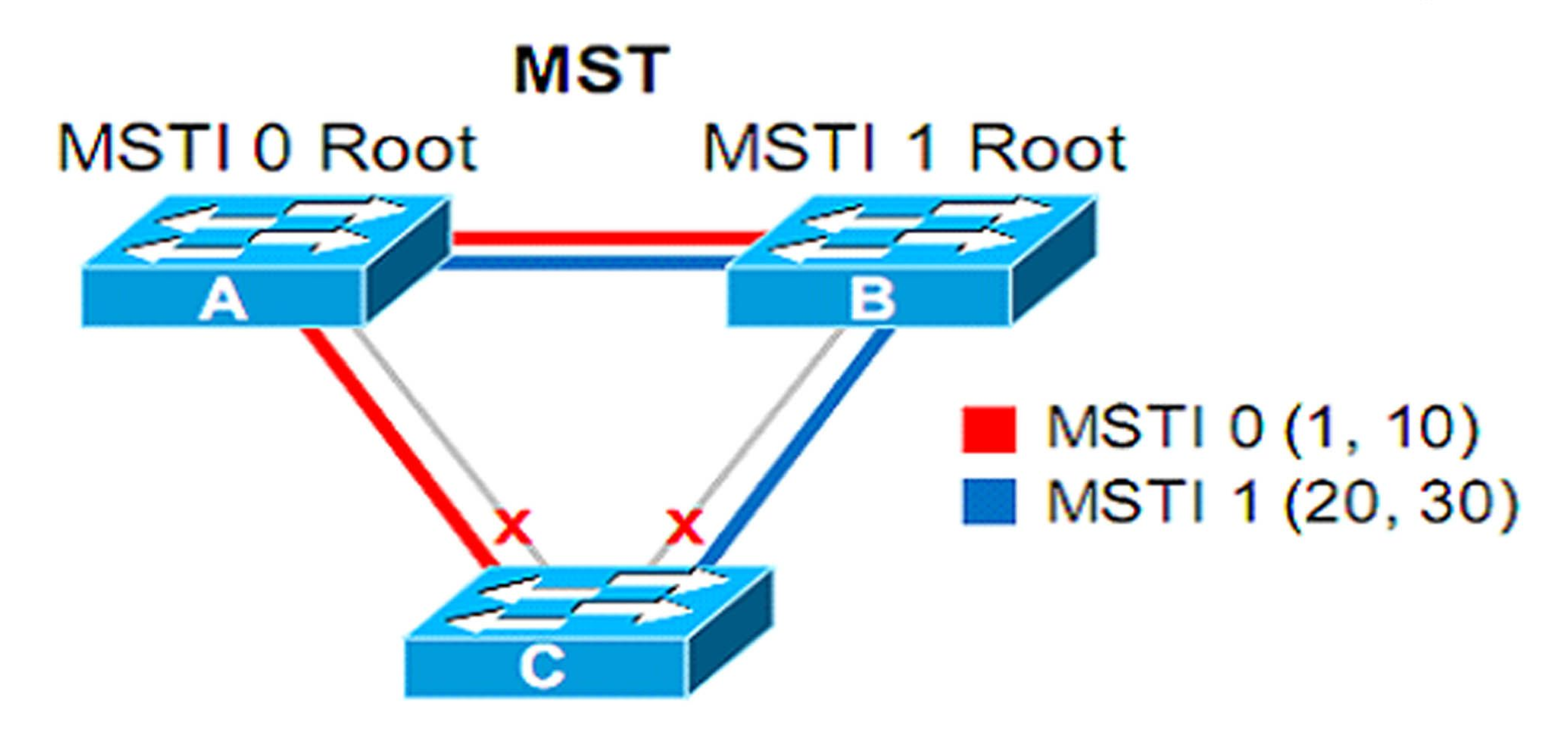
✻6 إستحداث مسميات جديدة خاصة بأنواع المنافذ الموجودة على السويتش مثل Edge Port وهي تعني أنه تم تفعيل خاصية الـFast Port على هذا البورت، والتى تقوم بتحويل البورت بشكل مباشر من الـDiscarding إلى Forwarding. وهي تستخدم عادة في البورتات التى لاتحوي سويتشات ممكن أن تؤدي إلى حدوث لووب في الشبكة أو مع أجهزة الكمبيوتر. بالإضافة إلى مسمى أخر وهو Shared Port، وهو يعني أن هذا البورت متصل مع HUP. وأخيرا مسمى جديد وهو Point-to-Point Port ويدل على أن البورت متصل مع سويتش أخر.

ملاحظة أخيرة وهي منذ عام 2004 تم أعتماد RSTP لكي يكون هو ال Default لل STPوتم تعريفه ب 802.1D وإحالة الـSTP للتقاعد، لذا عندما تسمع STP فكر بأنه RSTP.

MSTP: أو Multi Spanning Tree Protocol وهو معروف من قبل ال IEEE ب 802.1S.
فكرة هذا البروتوكول تهدف إلى تقليل عدد الـ Instances الموجودة بحيث نستطيع أن نضم أكثر من Vlan في Instance واحدة فكما ذكرت أن الـSTP سوف يقوم بعمل Instance لكل Vlan موجودة في الشبكة.

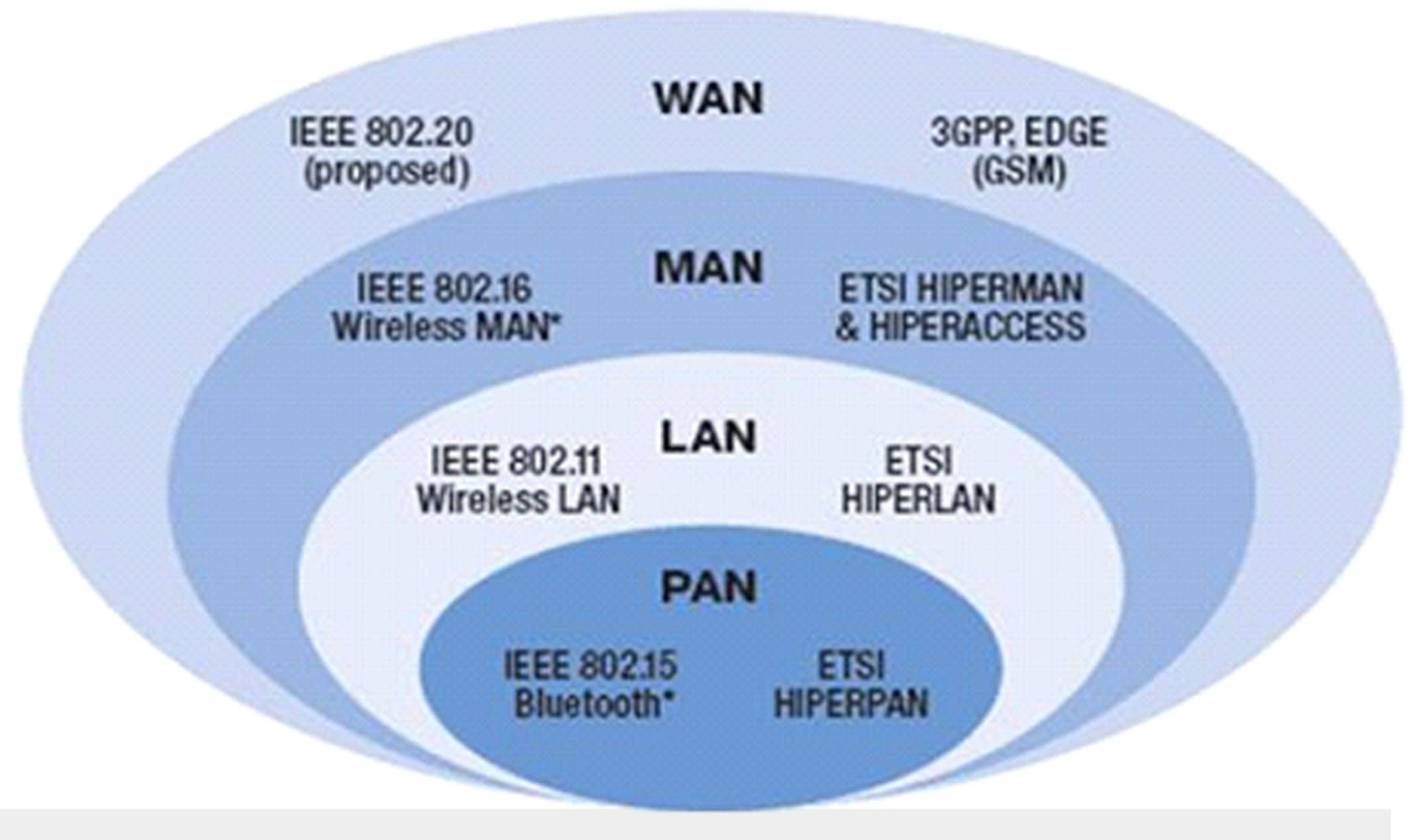
ومما لا شك فيه أن هذه العملية تخفف الضغط على المعالج كمنحى إيجابي لكنها سوف تمنع الشبكة من عمل Load Balancing بين ال Vlans كمنحى سلبي.

ومن هذا المنطلق وجد الـ MSTP الذي أتاح لنا تقسيم الـ Vlans على مجموعات تعمل كل منها بشكل مستقل عن الأخرى ومن خلال Instance منعزلة. وكمثال صغير حول هذه العملية لنفرض أن لدينا 40 Vlan في الشبكة وطبعا كل هذه ال Vlans سوف تعمل على شكل Instance واحدة كما ذكرنا في الSTP، لكن مع الـ MSTP الموضوع مختلف قليلا لأنه ببساطة سوف يسمح لنا بإنشاء Instance منفصلة لكل مجموعة منها. ولنفرض أن أول 10Vlans موجودة فى One Instance ، بينما باقي ال Vlans في Instance أخرى وبهذه الطريقة سوف يتم إغلاق منافذ معينة لكل مجموعة من الـ Vlans، بينما سوف تكون هذه المنافذ مفتوحة في المجموعة الأخرى. لاحظ معي الصورة القادمة لكي تفهم العملية بشكل أكبر:

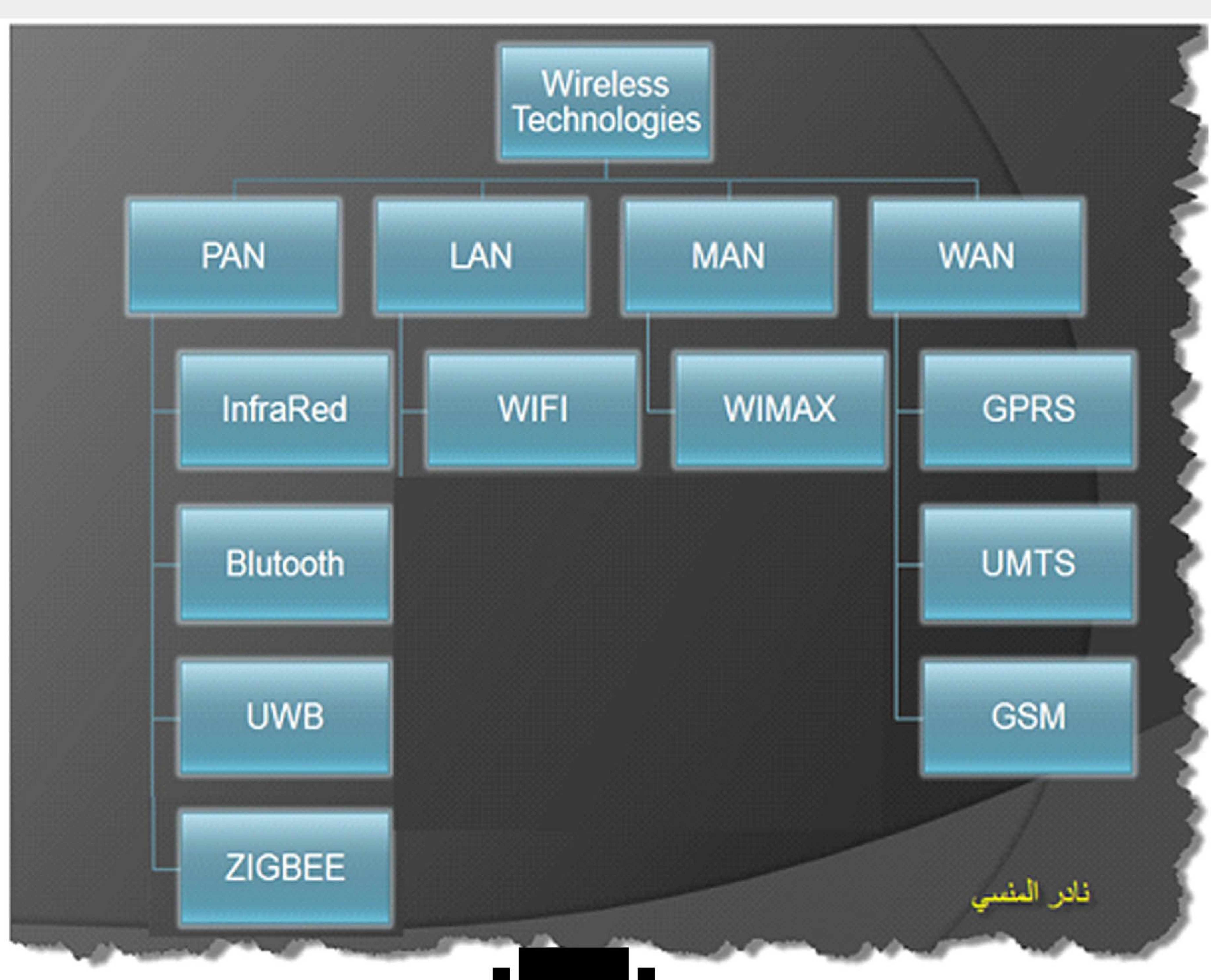


إلى هنا يكون الموضوع قد إنتهى على أمل أن نستكمل فيما بعد البروتوكولات الخاصة بسيسكو وهي PVST, PVST+ , RPVST والتى سوف أطرحها في العدد القادم إن شاء الله.

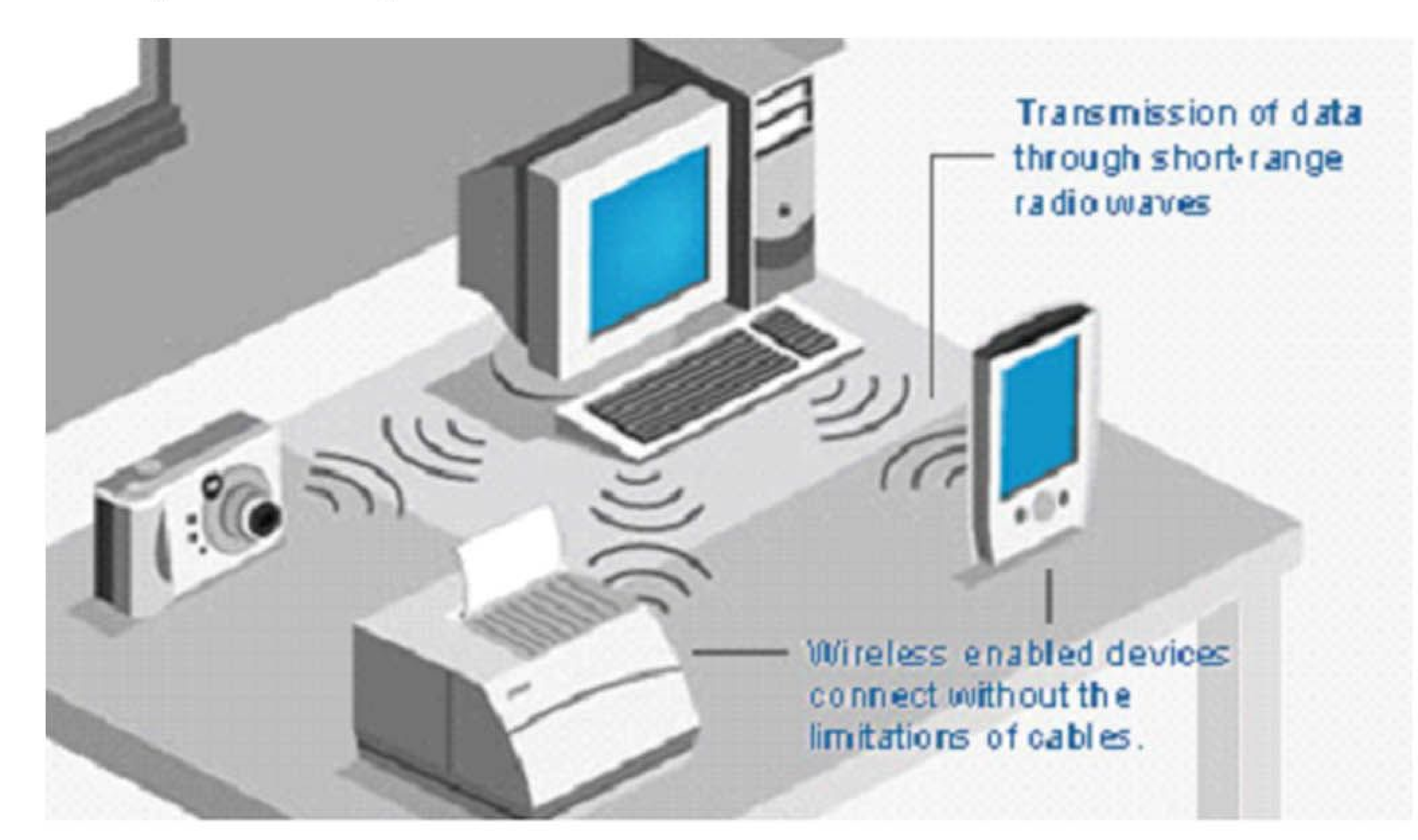
أيمن النعيمي



يتم تقسيم الشبكات اللاسلكية بنفس طريقة تقسيم الشبكات السلكية الي أربعة أنواع كل منها يتحدد حسب المساحة التي يغطيها و التي يستخدم في كل منها تقنية لاسلكية تتناسب مع المساحة التي تغطيها الشبكة و الشكل التالي يبين بعضا من التقنيات اللاسلكية الشبكية المستخدمة مقسمة تحت هذه الأنواع الأربع



الشبكات اللاسلكية الشخصية
(PAN (Personal Area Network

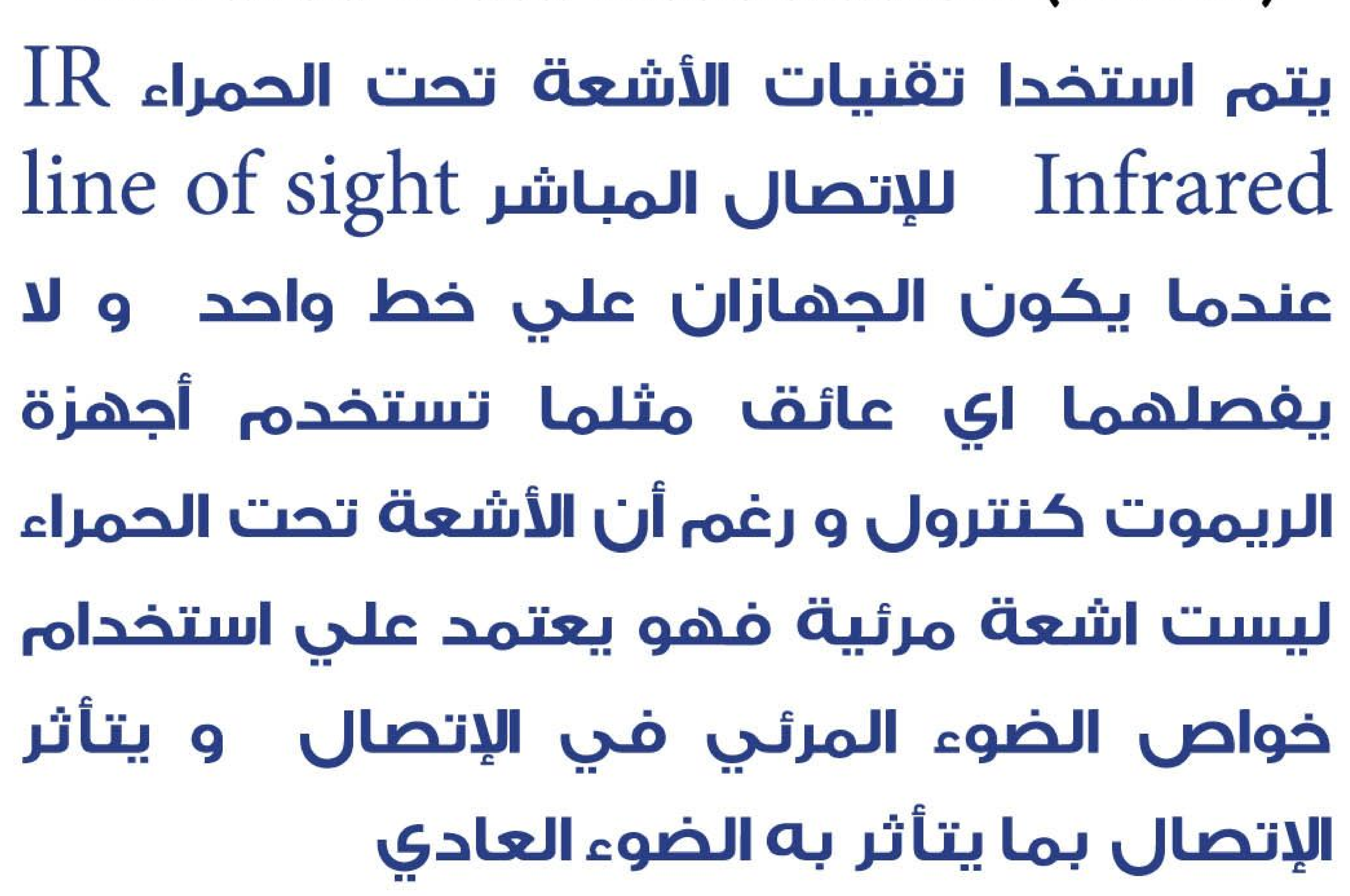




و هي تختص بالشبكات الشخصية علي مستوي متر الي عشرة امتار و تختص بالأساس في اتصال جهاز الكمبيوتر لاسلكيا ببعض الأجهزة الأخري الخدمية مثل الطابعات و الأكسس بوينت و السكانر و الكاميرات و أحيانا الماوس و الكيبورد

و تتميز هذه التقنية باستخدام ارسال لاسلكي بقدرة و طاقة محدودين لحصر حيز الإرسال في مكان صغير يستخدم في هذه الشبكات تقنيات شبك لاسلكي مثل IrDA, Bluetooth, UWB, Z-Wave , ZigBee

تقنيات الأشعة تحت الحمراء
Infrared Data Association (IrDA)



يتم استخدا تقنيات الأشعة تحت الحمراء IR Infrared للإتصال المباشر line of sight عندما يكون الجهازان علي خط واحد و لا يفصلهما اي عائق مثلما تستخدم أجهزة الريموت كنترول و رغم أن الأشعة تحت الحمراء ليست اشعة مرئية فهو يعتمد علي استخدام خواص الضوء المرئي في الإتصال و يتأثر الإتصال بما يتأثر به الضوء العادي



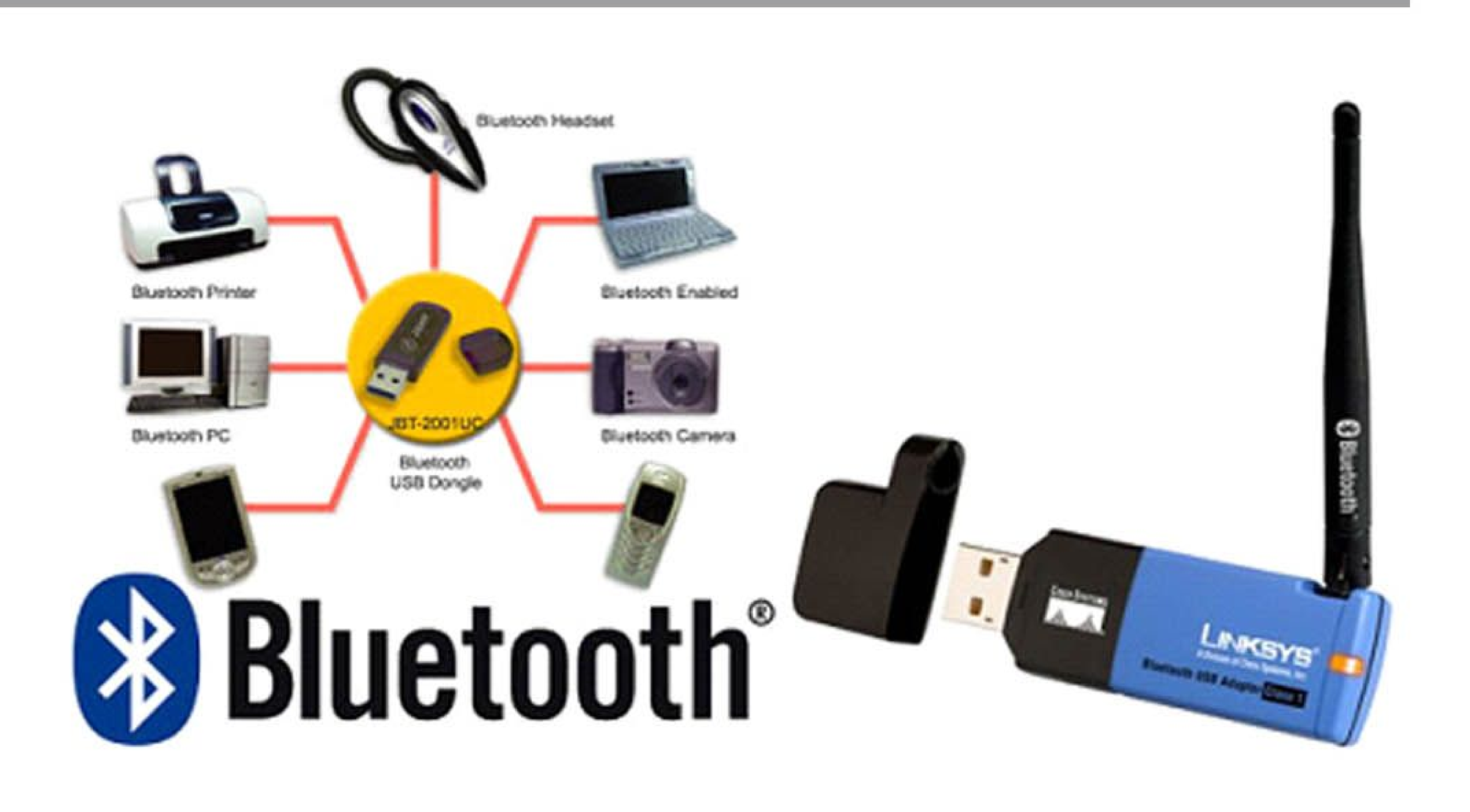




تقنية الإتصال اللاسلكي بواسطة البلوتوث
Bluetooth

عالجت هذه التقنية مشكلة اشتراط تواجد الأجهزة علي خط نظر واحد ومشكلة تعدد الإتصال و مشكلة الأمان و مشكلة السرعة حيث تستطيع أن تحقق الإتصال بين أكثر من جهاز في نفس الوقت مع توفر الأمان الشبكي

نادر المنسي

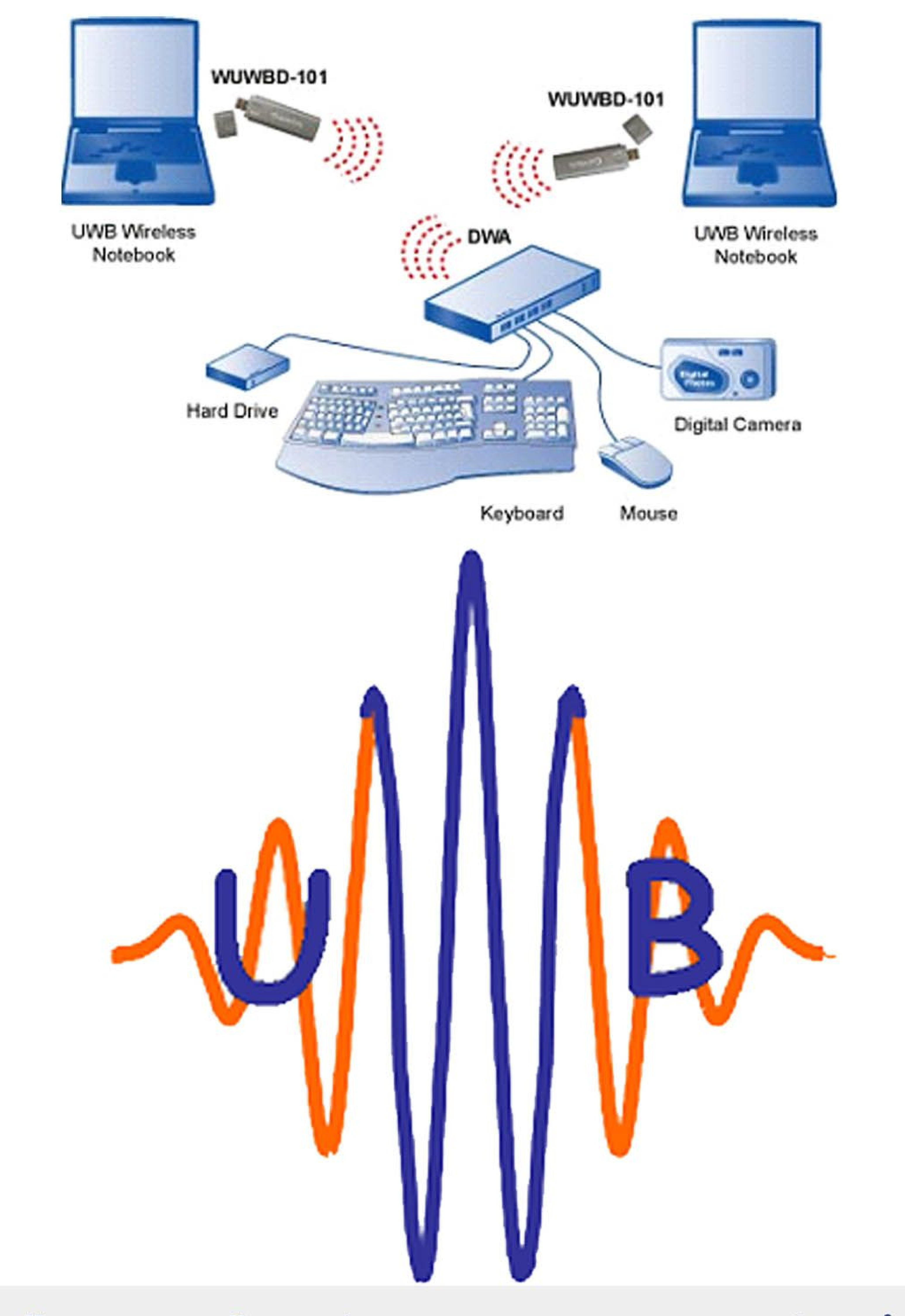


و كذلك ضمان سرعة تدفق للبيانات و يتم استخدام طريقة master / slave لعمل الإتصال و هي طريقة منظمة و عملية و منطقية للغرض الذي أنشيء له هذا النظام

تقنية البلوتوث تستخدم تردد ما بين 2.40 إلى 2.48 جيجاهيرتز و تقوم الأجهزة بتغيير التردد كل مرة اتصال و لذلك فمن الصعب جدا حدوث تداخل في الترددات بين الإتصالات

تقنية الإتصال اللاسلكي فائقة الإتساع

UWB Ultra-wideband



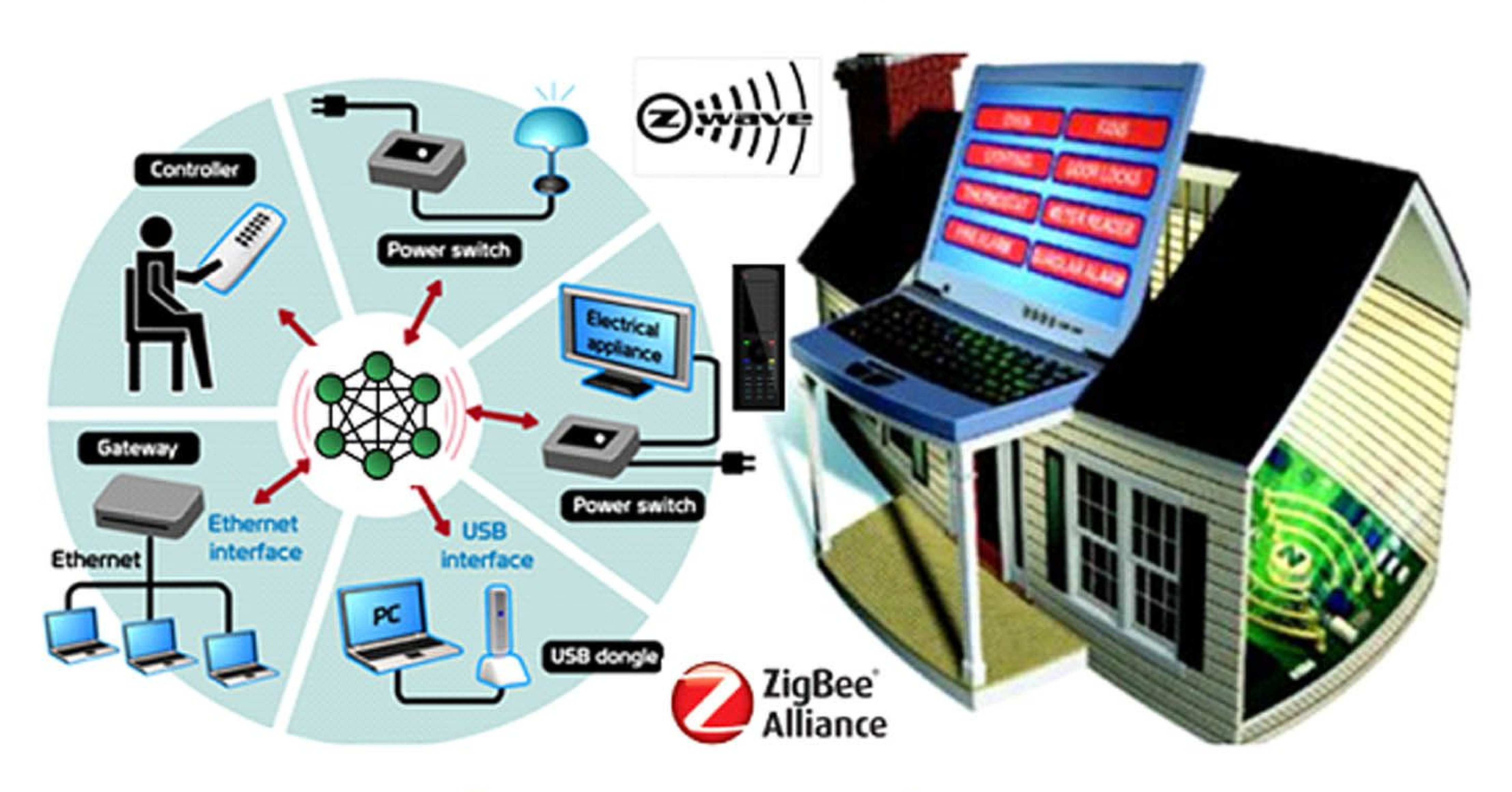
يعتبر الإتصال اللاسلكي فائق الإتساع من التقنيات الأحدث في عالم الإتصالات الشبكية اللاسلكية و الأعجب ايضا فهي تستخدم موجات راديوية واسعة النطاق ذات طاقة منخفضة جدا لإرسال بيانات كبيرة جدا و هذه الميزات قد تزيح جانبا اسماء عملاقة مثل البلوتوث و الواي فاي في الشبكات السالكية الشخصية

يبلغ سرعة نقل بيانات لاسلكيا تصل إلى أكثر من 480Mbps و هو هكذا أسرع عشرات المرات من معيار الواي الفاي 802.11b و تتميز معداته أيضا بما يتميز به معدات البلوتوث من توافقيته و أيضا قدرته علي العمل بتكنولوجيا التشغيل و التوصيل الآلي PNP و تتميز معداته ايضا بإمكانية ربطها بواسطة جهاز سويتش يعتمد علي تكنولوجيا UWB بما يجعله شبيها بأجهزة الواي فاي

يعتبر الإتصال اللاسلكي فائق الإتساع من التقنيات الأحدث في عالم الإتصالات الشبكية اللاسلكية و الأعجب ايضا فهي تستخدم موجات راديوية واسعة النطاق ذات طاقة منخفضة جدا لإرسال بيانات كبيرة جدا و هذه الميزات قد تزيح جانبا اسماء عملاقة مثل البلوتوث و الواي فاي في الشبكات السالكية الشخصية

يبلغ سرعة نقل بيانات لاسلكيا تصل إلى أكثر من 480Mbps و هو هكذا أسرع عشرات المرات من معيار الواي الفاي 802.11b و تتميز معداته أيضا بما يتميز به معدات البلوتوث من توافقيته و أيضا قدرته علي العمل بتكنولوجيا التشغيل و التوصيل الآلي PNP و تتميز معداته ايضا بإمكانية ربطها بواسطة جهاز سويتش يعتمد علي تكنولوجيا UWB بما يجعله شبيها بأجهزة الواي فاي

الإتصال و التحكم اللاسلكي عبر تقنيتي
Z-Wave /Zigbee



في هاتين التقنيتين سنتخطي حدود الشبكات الكلاسيكية التي تعتمد فقط علي الكمبيوتر و ملحقاته ,, فأنت هنا تستطيع أن تربط كل جهاز كهربي في بيتك بالشبكة (شبكة الواي فاي –معدات الإنترنت – التلفاز – المصباح – الثلاجة – الأبواب الكهربية – الغسالة – السخان – التكييف .. الخ)حيث تمكنك هاتين التقنيتين ومعداتهما من صنع شبكة تقوم بالتحكم بكافة أجهزتك الكهربية و الإلكترونية و ذلك لاسلكيا بواسطة برنامج تحكم علي الكمبيوتر و أجهزة الريموت كنترول

و علي عكس الشبكات العادية التي تحتاج أن يكون الجهاز مصنع مسبقا لينضم للشبكة فإنك هنا تستطيع ان تضم اي جهاز الكتروني او كهربي الي شبكة z-wave بواسطة وضع رقاقة تحكم لاسلكي خارجية لأي جهاز و ذلك بعملية تسمي "pairing" and "adding"

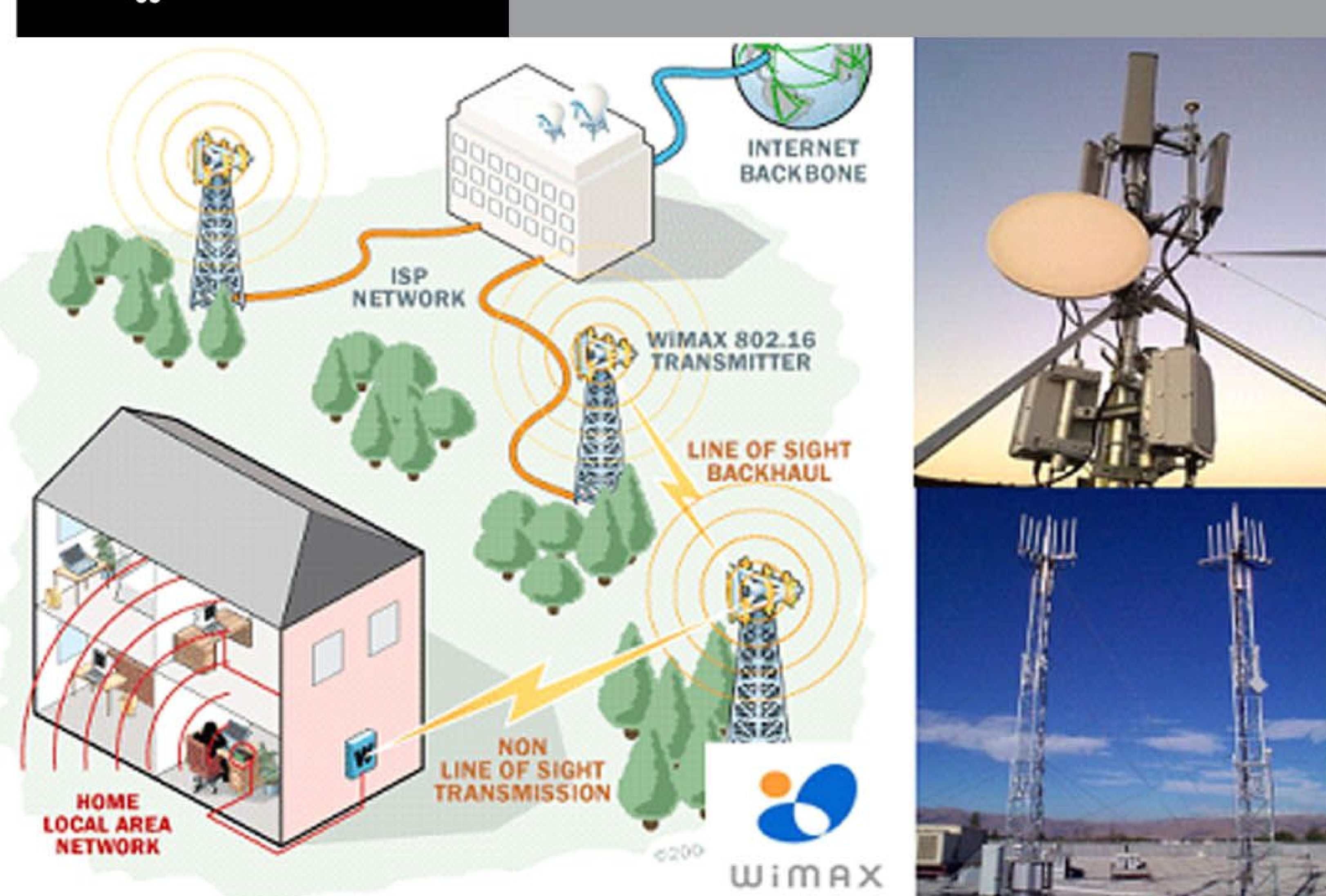
وكباقي الشبكات الشخصية فإنها تستخدم نطاق ترددي مجاني هو industrial, scientific and medical (ISM) و يستخدم بالأساس في الأجهزة الطبية و الصناعية و هذه الترددات تعمل بموجات ذات طاقة منخفضة علي مسافات قصيرة و علي عكس أجهزة البلوتوث فإن شبكة z-wave او zigbee تستطيع التحكم في ما يقرب من 232 جهاز تتواصل فيما بينها بتكنولوجيا أو طبولوجية طبولوجية source-routed mesh network حيث يكون هناك أكثر من جهة تستطيع التحكم في الشبكة و التخاطب مع أكثر من جهة

الشبكات اللاسلكية المحلية
WLAN (Local Area Network)

و هي أكثر الشبكات اللاسلكية انتشارا وشيوعا و هي تعتبر الشبكات المناظرة للشبكات السلكية الشائعة و تسمي أيضا الواي فاي WIRELESS FIDELITY WI Fi وهي خدمة الإتصال الشبكي لاسلكيا فائقة السرعة والدقة و يتم الدخول اليها عن طريق الكمبيوتر المحمول Notebook PC أو عن طريق الكمبيوتر الجيبي Pocket Pc مثل i mate او PDA أي " المساعد الرقمي الشخصي "







و توجد في المواقع العامة مثل الفنادق والمطارات والجامعات والمطاعم وأصبحت شركات الطيران تقدم هذه الخدمة على متن طائراتها. ومن المتوقع ان يصل مستخدمي هذه الخدمة الي 150 مليون شخص بنهاية عام 2011 م ان لم يصل بعد.

WMAN (Wireless Metropolitan Area Network)

شبكات المدن اللاسلكية

أصبح الغموض يكتنف مستقبل تكنولوجيا الواي ماكس بعد ان قامت عديد من الشركات بوقف خطوط انتاج معداتها و علي رأسها سيسكو و نوكيا , فلقد كانت و لازالت حتي الآن تكنولوجيا الواي ماكس مثال تطبيقي علي شبكات المدن اللاسلكية WMAN و كنا و لازلنا ننظر لها بكثير من الأمل متمنين يوما أن تحل مكان شبكات الواي فاي و نتخيل اننا سنتعامل مع الإنترنت و نتوغل فيه و كأننا نستخدم شبكة الموبايل

الواي ماكس أو Worldwide Interoperability for Microwave Access هي تكنولوجيا لاسلكية تستخدم المعيار 802.16 ieee لتوصي مقاييسها و تختلف عن سابقاتها ان المدي الترددي المستخدم لها مدفوع الأجر و لابد من اصدار تراخيص لها من الجهات المختصة

و تقدم غالبا بسرعات وسرعات خدمة الواي ماكس 512 كيلو بايت , 1024كيلو بايت , 2048 كيلو بايت و يتم بث الإرسال عبر أبراج لاسلكية تشبه أبراج الموبايل تخدم مناطق تزيد مساحتها عن مئات الكيلومترات و يتم استقبال الإرسال عبر هوائيات أطباق استقبالDESH علي ارتفاع ثلاثة امتار

الشبكات اللاسلكية الموسعة

WirelessWAN (Wide Area Network)

قبل أن أقول أن هذا الأمر واسع جدا احب أن أركز في ذهنك مبدأ مهم جدا و هو ان أي من التقنيات السابقة قد تتأرجح بين كونها شبكات محلية او مدن او واسعة حسب المنطقة التي تغطيها و لا يعتبر كونها ذات تقنية معينة أن نحكم عليها بهذه التقنية , فنحن نستطيع أن نصنع شبكة مدن بواسطة تقنية الواي فاي بل و واوسعة ايضا

بالسنبة للشبكة اللاسلكية الموسعة فهي تستخد غالبا عبر شركات الهواتف المحمولة و التي تستختدم الموجات اللاسلكية و كذلك الأقمار الصناعية و المهم فيها هو طريقة انتقال الأرسال بين عدة شبكات محلية أو مدن أو حتي شبكات فردية او شخصية

و لأن الخوض ي هذه الشبكات سينقلنا الي حيز أكبر لتوسعنا به فسنكتفي بذلك و هذا جدول مقارنة بين الشبكات اللاسلكية

	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11 HiperLAN2	802.11 MMDS, LMDS WiMAX (802.16)	GSM, GPRS, CDMA,HSDPA 2.5-3G-3.5G
Speed	< 1Mbps	11 to 54 Mbps	11 to 100+ Mbps	10 to 384Kbps 1.8/3.6 – 7.2Mbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	E1 replacement, last mile access	Mobile Phones, cellular data

معهد مهندسي الإلكترونيات والكهرباء IEEE 802

نادر المنسي

عندما تريد الولوج الي مجال وتكون متخصصا فيه فلابد ان تدرس المقاييس الخاصة به والإتفاقيات التي سطرت لتحديدها وان تتابع دوما المنظمات والهيئات المختصة به

وفي مجال الشبكات فإن معهد مهندسي الإلكترونيات والكهرباء هو المنوط به وضع تلك المقاييس و بدراستها تستطيع ان تتفهم كثيرا من ذلك المجال

فمثلا شبكات الواي فاي جزء من الشبكات اللاسلكية و التي بدورها جزء من الإتصالات و التي تنتمي بدورها الي فرع الإلكترونيات والكهرباء من الهندسة فإنه وجب البحث عن ما يخص الواي فاي في هذا المعهد

وما يخصنا كمهندسي شبكات في مقاييس هذا المعهد هي المقاييس التي تبدأ بتلك الصيغة IEEE 802.x وتستطيع ان تضع مكان حرف X اي رقم يتراوح بين 1 و 22

وكل رقم له تفريعات وفي مجموعها تشرح وتؤصل للشبكات السلكية واللاسلكية وانواع الكابلات وقيم الترددات وغيرها

هي بالفعل موسوعة لم اراد ان يفهم الشبكات هندسيا من وجهة نظر مهندسي الإتصالات والإلكترونيات

واليكم كل ما يخصنا كمهندسي شبكات في هذا المعهد



- IEEE **802.1** Bridging (networking) and Network Management
- IEEE **802.2** Logical link control (inactive)
- IEEE **802.3** Ethernet
- IEEE **802.4** Token bus (disbanded)
- IEEE **802.5** Defines the MAC layer for a Token Ring (inactive)
- IEEE **802.6** Metropolitan Area Networks (disbanded)
- IEEE **802.7** Broadband LAN using Coaxial Cable (disbanded)
- IEEE **802.8** Fiber Optic TAG (disbanded)
- IEEE **802.9** Integrated Services LAN (disbanded)
- IEEE **802.10** Interoperable LAN Security (disbanded)
- IEEE **802.11** Wireless LAN & Mesh (Wi-Fi certification)
- IEEE **802.12** demand priority (disbanded)
- IEEE **802.13** Cat.6 — 10Gb lan (new founded)
- IEEE **802.14** Cable modems (disbanded)
- IEEE **802.15** Wireless PAN
- IEEE **802.15.1** (Bluetooth certification)
- IEEE **802.15.4** (ZigBee certification)
- IEEE **802.16** Broadband Wireless Access (WiMAX certification)
- IEEE **802.16e** (Mobile) Broadband Wireless Access
- IEEE **802.17** Resilient packet ring
- IEEE **802.18** Radio Regulatory TAG
- IEEE **802.19** Coexistence TAG
- IEEE **802.20** Mobile Broadband Wireless Access
- IEEE **802.21** Media Independent Handoff
- IEEE **802.22** Wireless Regional Area Network

جمعية مهندسي الكهرباء و الإلكترونيات المحدودة. Institute of Electrical and Electronics Engineers, Inc. و إختصارها أي تريبل إي IEEE تلفظ (Eye – triple E) ، و هي جمعية محترفة تقنية لاربحية لما يقرب من نصف مليون عضو موزعين في معظم دول العالم. ، و هي جمعية معروفة و مشهورة جدا في الأوساط العلمية.

تشكلت IEEE في العام 1963 باندماج مؤسستي American Institute of Electrical Engineers التي تأسست عام 1884 ومؤسسة (Institute of Radio Engineers (IRE التي تأسست عام 1912.

تسعى IEEE إلى إختراع، تطوير، مشاركة وتطبيق المعارف المتعلقة بالإلكترونيات وتكنلوجيا❋

وفرت IEEE الدخول لملايين الوثائق التقنية مؤتمرات للبحث وتبادل الخبرات وعرض أخر الإختراعات ، فرص عمل بشركات عالمية ، وبعثات دراسية – هذا ما وجدته للآن

هناك 11 فرع إقليمي في 8 دول عربية ، و 40 فرع طلابي في 40 جامعة عربية "المعلومة منذ سنتين" و في عام 1999 تم تأسيس أول فرع للجمعية في فلسطين في الجامعة الاسلامية بغزة ، و قد حظى الفرع بالكثير من التأييد و الاهتمام من قبل محاضري و محاضرات كلية الهندية قسم الكهرباء و الحاسوب ، و لا يزال المكتب يقدم العديد من الخدمات للفئة الطلابية و تجدون تفصيل لنشاطات المكتب و خدماته في صفحة "نشاطاتنا" على الموقع.

من خلال مساهمة أعضائها، IEEE تمثل الجمعية المرجع الأساسي للكثير من المواضيع التقنية و التي تتراوح من هندسة الحاسوب، التقنية الطبية الحيوية والإتصالات، إلى الطاقة الكهربائية وهندسة الطيران والأجهزة الإلكترونية، و غير ذلك الكثير.

من خلال نشراتها التقنية، المؤتمرات والنشاطات فإن IEEE تنتج ما يقارب 30 بالمائة من النشر العلمي الخاص بالهندسة الكهربائية و الإلكترونية، و علم الحاسبات، كما تقيم سنوياً أكثر من 300 مؤتمر رئيسي و لها تقريباً 900 معيار قياسي مستعمل و ما يقارب الـ 500 تحت التطوير.

اذن فإن معهد المهندسين الكهربائيين والإلكترونيين من كبار مطوري المقاييس الدولية التي تقوم على أساسها الكثير من المنتجات والخدمات اليوم، وخاصة في مجال الاتصالات، وتكنولوجيا المعلومات، وتوليد الطاقة. ويعد معهد المهندسين الكهربائيين والإلكترونيين، بما لديه من مجموعة فعلية تحتوي على ما يقترب من 900 مقياس فعلي وأكثر من 400 مشروع تحت الإنشاء، المصدر الرئيسي للتوحيد القياسي في نطاق واسع من التكنولوجيات الواعدة، وهو يرحب بالمهندسين الفرديين والمؤسسات للمساهمة في أنشطته.

واليوم فإن سرعة تحرك بيئة الأعمال تتطلب التوحيد القياسي لضمان نمو السوق. وتدرك الشركات أنه من أجل تلبية التوقعات المتزايدة للعملاء، ولزيادة الربحية وتوسيع نطاق فرص السوق، من الأمور الهامة لضمان النجاح أن يتم الالتزام بتطوير وتنفيذ مقاييس معهد المهندسين الكهربائيين والإلكترونيين.

مجموعات معهد المهندسين الكهربائيين والإلكترونيين

❋ معهد المهندسين الكهربائيين والإلكترونيين – التطبيقات

❋ معهد المهندسين الكهربائيين والإلكترونيين – الاتصالات

❋ معهد المهندسين الكهربائيين والإلكترونيين – الكمبيوتر والإلكترونيات

❋ معهد المهندسين الكهربائيين والإلكترونيين – الأدوات والمصطلحات

❋ معهد المهندسين الكهربائيين والإلكترونيين – الطاقة

وهناك مجموعات اخر تستطيع تصفحها من هنا

http://www.ieee.org/web/societies/home/index.html

وتستطيع الإشتراك فيها ولكن بقيمة مدفوعة مقدما

❋ يحصل المشتركون على إمكانية الوصول الآمن عبر الإنترنت لخدمات البحث ، والاستعراض ، ووضع الإشارات المرجعية، والتتبع، وطباعة المستندات وفقاً لاتفاقية الترخيص. يتم تحديث المستندات يومياً. يمكن لعدة مستخدمين المشاركة في رخصة واحدة. تحصل أيضاً على إمكانية الوصول إلى البيانات الببليوغرافية لمقاييس IHS – أكثر من 1 مليون مستند.

موقع المعهد

http://www.ieee.org/web/membership/home/index.html



تحدثت في الجزء الأول من هذه المقالة في العدد الماضي عن الخطوة الأولى في عملية اكتشاف الأخطاء وإصلاحها وكانت عن جمْع المعلومات عن طريق التعرف على الأعراض والمشاكل الموجودة . واليوم سأتابع معكم شرح الخطوات التالية من الخطوات التسع لهذه المنهجية .

الخطوة (٢): تحديد الأماكن التي بها عطل في الشبكة

بعض المشكلات تكون متعلقة بمستخدم واحد وفي مكان واحد ، وهناك من المشكلات ما يؤثر على المئات أو ربما الآلاف من المستخدمين وتمتد في عدة أماكن . ولذلك فإن تحديد المنطقة المتضررة في الشبكة هي خطوة مهمة في عملية الإصلاح ، وغالبا ما تكون هذه الخطوة هي نقطة الانطلاق لرسم الاستراتيجيات التي ستستخدمها في حل المشكلة .

المشكلات التي تصيب عدد كبير من المستخدمين في وقت واحد هي مشكلات تتعلق بالاتصال غالباً ، و يمكن حصر مواقعها في كبائن الأسلاك (wiring rooms) ، أو في أجهزة الشبكة (network devices) مثل السويتشات و الراوترات ، أو في غرف السيرفرات (server rooms) . أما إذا كانت المشكلة تخص جهاز مستخدم واحد فإن عملية الإصلاح غالباً ما تبدأ و تنتهي بنفس مكان هذا الجهاز .

عندما يحدث عطل في الاتصالات عن مجموعة ما فإن ذلك سيقودك فعلاً إلى التوجه نحو كبينة الأسلاك أو إلى السيرفر ، ولكن ليس بالضرورة أن تبدأ عملية إصلاح المشكلة هناك ، لذا فإن معرفة من تأثر بهذا التعطل أولاً هي المعطيات الأولية عن مكمن وجود المشكلة بالضبط .

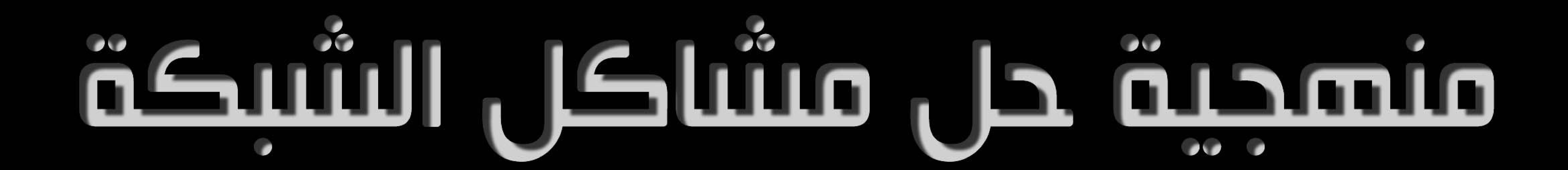
ولنأخذ مثالاً عمليا لتقريب هذه الفكرة . افترض أنك تقوم بإصلاح مشكلة اتصال جهاز مستخدم بالشبكة ، فأول ما يجب أن تبدأ به هو أن تذهب لجهاز العميل (client) وتقوم بعمل PING منه إلى السيرفر ، فإذا فشلت هذه التجربة حاول أن تكرر هذه العملية من الأجهزة الأخرى الموجودة في نفس الشبكة مع هذا الجهاز . إذا كانت عملية الـ PING في جميع الأجهزة غير ناجحة فإن عملية استكشاف الخطأ ومعالجة المشكلة سوف تنتقل إلى الشيء المشترك بين هذه الأجهزة ، أي السيرفر أو السويتش (switch) مثلاً .

المقابلة هي :

الخطوة (٣): معرفة آخر التغييرات في الشبكة

عندما تحدث مشكلة في اتصال جهاز ما بالشبكة أو قد تكون المشكلة في الشبكة ككل ، يجب أن تضع في الاعتبار أن ما قبل حدوث المشكلة كان كل شيء يعمل بشكل سليم . وكثيراً ما يتلقى قسم الدعم الفني تبليغاً بأن "الكمبيوتر توقف عن العمل" ، وهذا الإدعاء غير محبب نوعاً ما لأن من الأفضل القول أن هناك تغييرات حصلت في النظام أو في الشبكة أدّت إلى حدوث هذه المشكلة . و بناء على ذلك ، فإن تحديد ومعرفة ما تغيّر في الشبكة يمكن أن يقودك في الاتجاه الصحيح لحصر وحل المشكلة .

التغييرات يمكن أن تحدث في في أجهزة الشبكة ، أو السيرفرات ، أو في أجهزة المستخدمين . وسأوضح الآن هذه النقاط .





بسم الله الرّحمن الرّحيم التغييرات في أجهزة الشبكة

تإن إضافة أو إزالة أجهزة Hub أو Switch أو Server في الشبكة أو تغيير قيم معلومات الراوتر ، قد يؤدي إلى حدوث خلل في اتصالات الشبكة . ولذلك فإن أي تغيير في هذه الأجهزة سواء أكان فيزيائياً (physical) أو منطقياً (logical) فعلى مدير الشبكة توثيق ذلك بمستندات مع التفصيل الشامل . وبهذا ، فعندما تحدث أو يتكرر حدوث مشكلة ما في توبولوجية الشبكة فإنه يمكن الرجوع إلى هذه الوثائق وبالتالي حل المشكلة في أسرع وقت ممكن .

التغييرات في السيرفرات

يعتبر القيام ببعض الترقيعات والإصلاحات جزء من مهام مدير الشبكة ، وقد تؤدي هذه الترقيعات والإصلاحات أحياناً بالرغم من لزومها إلى مشكلات عديدة غير مقصودة . حتى أن أبسط الأعمال على السيرفر يمكن أن يكون لها تأثير سلبي على الشبكة .

ومن هذه الأعمال :

1❊ تغييرات في حسابات المستخدمين

2❊ تغييرات في صلاحيات المستخدمين

3❊ الترقيات والتحديثات لنظام السيرفر

4❊ تثبيت تطبيقات جديدة

5❊ تغييرات بـ هاردوير السيرفر

تغييرات في أجهزة المستخدمين

ليس كل التغييرات التي تتم على أجهزة المستخدمين تكون من تحكّم مدير الشبكة . فكثيراً ما يقوم بعض المستخدمين بتثبيت برمجيات بأنفسهم مثلاً .

ومثل هذه التغييرات يمكن أن ينتج عنها مشاكل تكون صعبة الحل إلى حد ما حيث أن كثيراً من المستخدمين لا يتوقعون نتيجة تلك التغييرات التي قاموا بها على أجهزتهم .

